

## PROPRIETARY INFORMATION AGREEMENT

Effective as of the last date of execution written below (the “Effective Date”), SINTAVIA, LLC (“SINTAVIA”), a Delaware limited liability company, with offices at 2500 SW 39<sup>th</sup> Street, Hollywood FL 33312, USA, and \_\_\_\_\_ (“Company”) a \_\_\_\_\_, with offices at \_\_\_\_\_, agree to the following terms and conditions for the protection, use and disclosure of Proprietary Information. SINTAVIA and Company are referred to individually as a “Party” and together as the “Parties”.

1. Purpose. In order that the Parties may discuss one or more business opportunities that may be of interest to them, making it necessary or desirable to exchange, disclose, or permit access to the Proprietary Information, this Agreement provides for the protection against unauthorized use and disclosure of Proprietary Information that may be disclosed by each Party relating to a potential transaction involving SINTAVIA and Company (the “Purpose”).

2. Definition of Proprietary Information. Each Party shall protect the other Party’s Proprietary Information in accordance with the terms of this Agreement. For purposes of this Agreement, Proprietary Information means: all information, whether written, oral or observed, whether or not marked or identified as “proprietary” or “confidential” made available by or on behalf of a Party with respect to its or its affiliates’ business, assets, financial condition, operations and prospects, together with any and all analyses, compilations, studies or other documents, materials or records prepared by either Party or any of their representatives which contain or otherwise reflect or, in whole or in part, are generated or derived from, any of the foregoing.

3. Designated Representative. Each Party agrees to designate in writing a specific individual as the point of contact for disclosing and/or receiving written Proprietary Information transmitted between the Parties.

4. Protection of Proprietary Information. The receiving Party shall use Proprietary Information received from the disclosing Party under this Agreement only in support of the Purpose, and shall preserve and protect such Proprietary Information from disclosure to any third party (including patent offices), through an exercise of care equivalent to the degree of care it uses to preserve and protect its own Proprietary Information, but, in any event, with no less than a reasonable standard of care for protection. In addition to the foregoing, the receiving Party shall not (i) analyze the disclosing Party’s samples to determine their composition, or (ii) measure the properties of the disclosing Party’s samples, except as reasonably necessary to accomplish the Purpose. Notwithstanding the foregoing, the receiving Party may disclose the disclosing Party’s Proprietary Information to its employees, contractors, advisors and counsel (“Representatives”) who both (x) require that access in order to achieve the Purpose and (y) have been made aware of this Agreement and are subject to this Agreement or to confidentiality obligations to the receiving Party that are no less restrictive than those in this Agreement. Each Party shall be liable for its Representatives’ compliance with the terms of this Agreement.

5. Exceptions to Liability for Disclosure. Proprietary Information shall not include information that: (a) is, at the time of disclosure, already in, or later falls into, the public domain through no act or omission on the part of the receiving Party, its directors, officers, employees, or agents; or, (b) was known to the receiving Party at the time of disclosure as documented by the receiving Party’s previously existing written records; or, (c) is disclosed to the receiving Party with the prior written approval of the disclosing Party; or, (d) is independently developed by the receiving Party subsequent to its receipt, as substantiated by reasonable documentation without use of or reference to the Proprietary Information of the other Party; or,

(e) is in the possession of the receiving Party or is later obtained by the receiving Party in writing and without any restrictions on further disclosure from a third party which was legally entitled to disclose same and which did not acquire same from the Party claiming the proprietary interest. If the receiving Party is required to disclose any Proprietary Information pursuant to judicial action or other legal or regulatory demand, such disclosure shall not violate this Agreement; provided, (i) the receiving Party notifies the disclosing Party so that it is afforded an opportunity to prevent or limit such disclosure; (ii) the receiving Party reasonably cooperates with the disclosing Party's efforts under subparagraph 5(i) above; and (iii) the receiving Party ensures that the disclosure is made only to the extent legally required.

6. Duration and Termination. This Agreement shall terminate three (3) years after the Effective Date herein, unless sooner terminated by a Party by giving thirty (30) days written notice to the other Party. Termination shall not, however, affect the rights and obligations contained herein with respect to Proprietary Information supplied hereunder prior to termination, which shall remain subject to the confidentiality obligations of this Agreement for a period of five (5) years after the termination date of this Agreement (the "Confidentiality Period"), except for Proprietary Information constituting a trade secret under applicable law, in which case such Proprietary Information shall remain subject to the confidentiality obligations of this Agreement for as long as it qualifies as a trade secret. Upon termination of this Agreement, the Proprietary Information received hereunder may be retained by the receiving Party for archival purposes only pursuant to routinely held record retention policies or, at the request of the disclosing Party, returned, deleted or destroyed and a certificate of deletion or destruction provided to the disclosing Party. However, if the Proprietary Information is retained by the receiving Party, it must be protected in perpetuity against unauthorized use or disclosure in accordance with this Agreement for as long as it is retained, unless the disclosing Party indicates otherwise in writing. This provision shall survive termination of this Agreement. Upon termination, or otherwise upon request, each Party shall either return to the disclosing Party or destroy all Proprietary Information received under this Agreement.

7. Derivative Information. For purposes of this Agreement, "Derivative Information" means any inventions, discoveries, improvements, designs, methods, devices, systems, works of authorship, or other non-public information generated by the receiving Party, whether solely or jointly with others, based on or derived from any Proprietary Information of the disclosing Party and/or its Affiliates. The receiving Party shall promptly disclose to the disclosing Party all Derivative Information. Derivative Information shall be considered to be the Proprietary Information of the disclosing Party and to be the disclosing Party's sole and exclusive property, subject to the protections afforded hereunder. The receiving Party agrees to assign, and hereby does assign, all right, title, and interest in and to Derivative Information to the disclosing Party. The receiving Party agrees to take such action and execute, and to require any of its employees to take such action execute, any and all documents reasonably necessary to perfect, secure and enforce the receiving Party's ownership of all such Derivative Information. In the event the receiving Party claims that such Derivative Information, or any portion thereof, was known to the receiving Party prior to disclosure by the disclosing Party or was developed without the benefit of the disclosing Party's Proprietary Information, the receiving Party shall have the burden of showing such by tangible evidence.

8. Licenses; Warranty.

(a) Neither the execution of this Agreement nor the furnishing of any Proprietary Information hereunder shall be construed as granting, either expressly or by implication, or otherwise, any license under any Derivative Information, Proprietary Information or other intellectual property now or hereafter owned by or controlled by the disclosing Party.

(b) The disclosing Party warrants that it has the right to disclose Proprietary Information hereunder for the Purpose. None of the Proprietary Information which may be submitted or exchanged by the Parties shall constitute any representation, warranty, assurance, guarantee, or inducement by a Party to

the other Party with respect to the infringement of patents, copyrights, trademarks, trade secrets, or any other rights of third persons. EXCEPT FOR THE FOREGOING, NEITHER PARTY MAKES ANY WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO INFORMATION FURNISHED TO THE OTHER HEREUNDER INCLUDING, WITHOUT LIMITATION, NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, FREEDOM FROM DEFECTS, FREEDOM FROM TRADE SECRET, PATENT OR COPYRIGHT INFRINGEMENT, ADEQUACY, ACCURACY OR SUFFICIENCY.

9. Restrictions on AI Systems. For purposes of this paragraph 9, the following terms have the following meanings: “Artificial Intelligence” or “AI” means technology that can make decisions, recommendations or predictions, generate content, recognize patterns, or act with no or limited human involvement to influence a real or virtual environment, without being explicitly programmed to do so; “AI System” means any software, algorithm, model, tool, or other capability that uses Artificial Intelligence, whether hosted on premises, in the cloud, or as a service; and “AI System Provider” means any third party that supplies, hosts, operates, or otherwise makes available an AI System for a Party.

(a) No AI System Training. The receiving Party shall not use any Proprietary Information or of the other Party, or any derivative thereof, for the training, retraining, testing, evaluation, validation, or development of any AI System.

(b) Limited AI System Use. Subject to paragraph 9(a) above, the receiving Party may only use the other Party’s Proprietary Information, or any derivative thereof, as an input to an AI System when: (i) the AI System is accessible only by the receiving Party, the other Party, and, if applicable, the AI System Provider; and (ii) the disclosing Party’s Proprietary Information is (x) not disclosed or otherwise accessible to any third party, including the AI System Provider, and (y) not stored, logged, cached, or otherwise retained by the AI System.

(c) Output of AI Systems. The receiving Party shall treat any output of an AI System that was based on inputs containing the other Party’s Proprietary Information, or any portion or derivative thereof, as the other Party’s Proprietary Information, including applying the original marking(s) (if any) to such output. The receiving Party shall notify the other Party in the event any output (or other product or material, including data) is developed via an AI tool.

(d) Documentation of use with AI Systems. The receiving Party shall maintain documentation of the use of the other Party’s Proprietary Information in any AI System and shall provide such documentation to the other Party promptly upon request.

10. Information Security.

(a) Definitions:

(i) “Countermeasures” means actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an Information System (as defined below).

(ii) “Information System” means a discrete set of information resources that collect, process, maintain, use, share, disseminate, or dispose information.

(iii) “Information Security Incident” means (A) any actual or suspected incident involving a Party’s Information System that may involve the disclosing Party’s Sensitive Information (as defined below), or (ii) any actual or suspected unauthorized access to, use, or disclosure of the disclosing Party’s Sensitive Information.

(iv) “Sensitive Information” means Proprietary Information, personal information, export-controlled information, Federal Contract Information as defined in FAR 52.204-21. Covered Defense Information as defined in DFARS 252.204-7012 and Controlled Unclassified Information (CUI) as defined in the National Archives and Records Administration (NARA) Registry.

(b) Reasonable and Appropriate Security Controls:

(i) Each Party shall apply reasonable and appropriate administrative, technical, physical, organizational, and operational safeguards and operations, including Countermeasures, to protect Sensitive Information against accidental and unlawful destruction, alteration, and unauthorized or improper disclosure or access regardless of whether such Sensitive Information is on a Party’s internal systems or a cloud environment.

(ii) If a Party’s performance of the Agreement involves the transmission, storage, or processing of Sensitive Information on an Information System, then Company shall, at a minimum, apply the following security controls:

A. Limit Information System access to authorized users, processes acting on behalf of authorized users, or devices (including other Information Systems).

B. Limit Information System access to the types of transactions and functions that authorized users are permitted to execute.

C. Verify, control and limit connections to and use of external Information Systems.

D. Control information posted or processed on publicly accessible Information Systems.

E. Identify users, processes acting on behalf of users, or devices.

F. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational Information Systems.

G. Sanitize or destroy Information System media containing Sensitive Information before disposal or release for reuse.

H. Limit physical access to organizational Information Systems, equipment, and the respective operating environments to authorized individuals.

I. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

J. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational Information Systems) at the external boundaries and key internal boundaries of the Information Systems.

K. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

I. Identify, report, and correct Information and Information System flaws in a timely manner.

M. Provide protection from malicious code at appropriate locations within Information Systems.

N. Update malicious code protection mechanisms when new releases are available.

O. Perform periodic scans of the Information System and real-time scans of files from external sources as files are downloaded, opened, or executed.

P. Establish and enforce security configuration settings for information technology products employed in the other Party's Information Systems.

Q. Establish and maintain data protection processes and systems to adequately protect Sensitive Information, including pertaining to destruction methods employed, how audit and system log information is protected, and having the capability to encrypt Sensitive Information during transmission.

R. Ensure that risks identified in scans performed under sub-paragraph (b)(2)(O) of this paragraph are promptly addressed.

S. Each Party shall comply with 48 C.F.R. 252.204-7012 when Covered Defense Information is disclosed.

c. Information Security Incident Response and Notification:

(i) Each Party must have documented processes that address Information Security Incidents. These processes should be a set of written instructions and Countermeasures that include, but are not limited to detecting, responding to, and limiting the effects of an Information Security Incident.

(ii) Within a reasonable time of discovery, the impacted Party will notify the non-impacted Party of the Information Security Incident. Specifically, Company shall notify SINTAVIA'S designated representative. At the impacted Party's expense, the impacted Party will (i) immediately investigate any Information Security Incident, (ii) make all reasonable efforts to secure Proprietary Information and mitigate the impact of the Information Security Incident, (iii) provide timely and relevant information to the non-impacted Party about the Information Security Incident on an ongoing basis, and (iv) cooperate as applicable with the non-impacted Party to provide notice to affected third parties.

(iii) This paragraph does not relieve either Party of any other applicable safeguarding requirements, remedies, or obligations regarding the protection of Sensitive Information required by this Agreement or local, federal, state, or other governmental agencies or departments, including but not limited to FAR 52.204-21 or DFARS 252.204-7012.

11. Relationship of Parties. Nothing in this Agreement shall grant to a Party the right to make commitments of any kind for, or on behalf of, another Party. This Agreement is not intended to be, nor shall it be construed as, a joint venture, teaming relationship, partnership, or other formal business arrangement, and no Party shall have the right or obligation to share any of the profits or bear any of the losses of another

Party under any contract or subcontract performed in conjunction herewith. This Agreement shall not be construed in any manner to be an obligation to enter into a definitive agreement or subcontract.

12. Export Compliance. Each Party shall comply with all applicable export control laws and regulations, including but not limited to the Arms Export Control Act, International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), including obtaining any licenses or permits thereunder and any other applicable government directives related to export control. Neither Party shall transfer any export-controlled information (e.g., technical data) from the U.S. to any non-U.S. person, country, government, or entity without first complying with all the requirements of the ITAR or EAR, as applicable. Any Party requesting U.S.G. authorization to export export-controlled information provided by the other Party under this Agreement must first obtain the disclosing Party's written consent. Written consent by the disclosing Party, however, shall not relieve the other Party of its obligations to comply with U.S. Export Regulations. Any product (to include data) developed via an AI tool and subject to export controls must be properly marked by the disclosing Party.

13. Applicable Law. This Agreement shall be governed by and construed in accordance with the internal laws of the State of Florida, without giving effect to any choice or conflict of law provision or rule (whether of the State of Florida or any other jurisdiction). Venue for any legal action or proceeding arising in connection with this Agreement shall be exclusively within the federal and state courts located in Broward County, Florida.

14. Limitation of Liability. EXCEPT FOR DAMAGES RESULTING FROM BREACH OF THE WARRANTY IN PARAGRAPH 9(b), THE DISCLOSING PARTY SHALL NOT BE LIABLE TO THE RECEIVING PARTY FOR ANY DAMAGES THAT MAY RESULT FROM THE RECEIVING PARTY'S RECEIPT OR USE OF, OR RELIANCE ON INFORMATION FURNISHED HEREUNDER, REGARDLESS OF WHETHER THE DISCLOSING PARTY WAS AWARE OF THE POSSIBILITY OF SUCH DAMAGES OR NOT, NOR SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE OR MULTIPLE DAMAGES ARISING FROM SUCH RECEIPT, USE, OR RELIANCE. HOWEVER, THIS LIMITATION OF LIABILITY FOR INDIRECT DAMAGES AND LOSSES WILL NOT APPLY WHERE THE RECEIVING PARTY HAS BREACHED THIS AGREEMENT. Any and all costs or expenses incurred by a Party arising from its performance of this Agreement shall be borne by the Party which incurred same, and no Party shall be liable or obligated to the other Party for said costs or expenses. Notwithstanding the foregoing, in the event any proceeding or lawsuit is brought by a Party against the other Party for violation of obligations under this Agreement, the prevailing Party shall be entitled to recover its costs and reasonable attorneys' fees from the other Party.

15. Entire Agreement. This Agreement contains the entire understanding between the Parties relative to the protection of Proprietary Information to be exchanged between the Parties for the Purpose, and supersedes all prior and collateral communications, reports, and understandings between the Parties with respect to such Purpose. No change, modification, alteration, or addition to any provision hereof shall be binding unless in writing and signed by authorized representatives of both Parties. This Agreement shall apply in lieu of and notwithstanding any specific legend or statement associated with any Proprietary Information exchanged, and the duties of the Parties with respect thereto shall be determined exclusively by this Agreement. If any portion of this Agreement is held to be invalid, such decision shall not affect the validity of the remaining portions.

16. Authority of Representatives. Each person, executing this Agreement, represents and warrants that each has full authority to enter into this Agreement on behalf of his/her company, and that each has been delegated the authority to bind his/her company in this Agreement.

17. Assignment; Successors and Assigns. This Agreement may not be assigned without the prior written consent of the other Party and any attempt to do so in violation of this paragraph 17 shall be null and void. This Agreement shall be binding upon and shall inure to the benefit of the Parties hereto, their successors and assigns. The waiver of any provision in any instance shall not be construed as a waiver in all other instances.

18. Equitable Remedies. It is understood and agreed by both Parties that money damages may not be a sufficient remedy for breach of this Agreement and that each Party shall be entitled to pursue specific performance, injunctive or other equitable relief as remedies for any such breach, at such Party's sole expense, without posting any bond or proving any damages. Such remedies shall not be deemed to be the exclusive remedies for the breach of this Agreement but shall be in addition to all other remedies available to the nonbreaching Party at law or in equity.

19. Release of Information or Advertising. During the Confidentiality Period, neither Party shall make any announcement or communicate any information to any third party concerning this Agreement without the prior written approval of the other Party. In addition, neither Party shall release to anyone outside its organization any information, or confirmation or denial of same, with respect to this Agreement or the subject matter hereof without the prior written approval of the other Party. Requests for approval shall be made at least fifteen (15) calendar days before the proposed date for release and shall identify the specific information to be released, the medium to be used, and the purpose for the release.

20. Remedy for Unauthorized Patent Obtention. This Agreement prohibits certain patent-obtention activities. If either Party or its affiliates (collectively the "Filing Party") files or prosecutes any patent application, or issues any patent, contrary to this Agreement, the Filing Party hereby agrees to grant, and hereby grants, to the other Party and its affiliates (collectively the "Other Party") a nonexclusive, worldwide, royalty-free immunity from suit under those patent applications and patents, together with the right to grant nonexclusive immunities from suit to third parties without accounting to the Filing Party, in addition to any other remedy available to the Other Party for that breach. Each Party agrees not to invoke any "statute of limitations" or similar legal or equitable device to suppress proof of such a breach, or to avoid enforcement of those immunities from suit. This Section survives termination of this Agreement.

[signatures follow]

**IN RECOGNITION OF THE ABOVE**, the Parties have caused this Agreement to be executed on the dates set forth below.

SINTAVIA, LLC

[Company]

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: Brian R. Neff

Name:

Title: Chief Executive Officer

Title:

Date: \_\_\_\_\_

Date: \_\_\_\_\_