WEST VIRGINIA EXECUTIVE BRANCH CONFIDENTIALITY AGREEMENT

This Confidentiality Agreement, including any attachments, (hereafter called "Agreement") is entered into between the State of West Virginia ("State") and the undersigned employee or contractor ("User").

This Agreement notifies the User of the policy and the User's responsibility to secure confidential information the State collects, possesses, uses and discloses. Additionally, the Agreement clarifies the user's obligations to limit their access, use, and disclosure of confidential information and to protect confidential information from unauthorized disclosure. Accordingly, the State prioritizes protecting the privacy, confidentiality, integrity, and availability of information, in all forms.

The User agrees as follows:

1. Definitions:

a. **Confidential Information:** Includes all information that is, or can be, classified as restricted or sensitive per the West Virginia Office of Technology's Data Classification Policy WVOT PO1006. Confidential information also includes personally identifiable information (PII) and all information designated confidential by law, rule, policy, or procedure. Confidential information may be processed on paper, electronically, and verbally, as well as in images. Examples include, but are not limited to, passwords and access codes; citizen, client, demographic, employee, medical, and taxpayer information; trade secrets; and security audits.

b. **Disclosure:** The access, release, transfer, sale, divulgence, or communication of information, in any manner, to any individual or entity other than the subject of the information, designated user, or information owner, in accordance with policy, as may be amended.

c. **Need to Know:** The principle that a User must only access the minimum amount of information necessary to perform a legitimate work-related task or function.

d. **Personally Identifiable Information (PII):** Information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information (PHI) as that term is defined below. PII is contained in public and non-public records. Examples include an individual's:

first name (or initial) and last name (current or former); geographical address; geolocation; electronic address (including an email address); cell number, landline phone number, and fax number, if dedicated to an individual at their place of residence; social security number; credit and debit card numbers; financial records, including payment history, and checking, savings, loan, and other financial account numbers; consumer report information; mother's maiden name; biometric identifiers, including but not limited to fingerprints, palm prints, voice prints, DNA, and face and iris scans; physical description; driver's license number; birth date; birth, adoption or death certificate numbers; medical, disability, or employment records, including salary information; computer information, including information collected through an internet cookie; and criminal records. PII includes any other information concerning an individual that, if disclosed, identifies, or can be used to identify or locate an individual physically or electronically.

e. **Protected Health Information (PHI):** A subset of PII and defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (*see* 45 C.F.R. §106.103), and only applies to entities that are covered by HIPAA. PHI consists of health information combined with individually identifiable information processed by HIPAA covered entities. Examples include physical and mental health status, diagnoses, treatment, medical supplies, demographic information, or payment for health services or medical supplies. PHI may be in electronic, paper or verbal form, and applies to the past, present, or future provision of health services and payments.

   Protected Health Information does not include records covered by the Family Educational Right and Privacy Act, 20 U.S.C. 1232g, and employment records held by the entity in its role as employer.

f. **Use:** The access, utilization, employment, application, examination, or analysis of information.

g. **Workforce:** Employees, volunteers, trainees, contract employees and other people whose conduct, in the performance of work for the State, is under the control of the State, whether or not the State pays them.

h. Other terms, not defined herein, are defined according to the definitions within the Privacy Policy Definitions, currently located at www.privacy.wv.gov.

2. Treatment of Confidential Information:

a. The User must access, collect, retain and use confidential information in conformity with policy and for legitimate work related purposes.

b. The User must not access, use or disclose confidential information for personal or non-work related purposes.

c. The User must not disclose any confidential information, unless the disclosure is made pursuant to law and policy, or the individual who is the subject of the confidential information consents to the disclosure in writing.

d. When confidential information is disclosed, care should be taken to prevent the redisclosure of that information to unauthorized persons or entities.

e. The User must protect confidential information from unauthorized collection, use, access, transfer, sale, disclosure, alteration, retention, or destruction whether accidental or intentional and must take necessary precautions to secure such confidential information to the extent possible. Accordingly, the User must not forward emails including confidential information to personal email addresses.

f. Where laws and policies do not exist to define and govern authorized access, use, or disclosure of confidential information, the User must receive prior approval from an appointed State counsel, designee, or authorized workforce member before accessing, using, or disclosing the information. All of the above applies to the information in total or fragmented form.

g. The User must not misuse or alter documents, media, forms, devices, or certificates in any manner which might compromise confidentiality or security, violate policy, or be illegal.

h. The User has no ownership rights to, or interest in, any information owned by or in the custody or control of the State. This includes any document, report, study, article or other written information prepared by the User as a member of the workforce; any software, computer equipment, or information technology; or any other property including copyrighted materials, except as specifically consented to by the State.

i. The User must report incidents, or suspected incidents, involving any unauthorized access, use, or disclosure, pursuant to the Response to Unauthorized Disclosures procedure located at www.privacy.wv.gov.

j. The User's access to confidential information is at the sole discretion of the State, and may be monitored, audited, modified, suspended, or terminated at any time.

k. The User should contact their immediate supervisor, agency privacy officer, or department privacy officer with any questions about this Agreement or classification of confidential information.

l. The User must comply with this agreement and the State's privacy and security policies. Compliance is a condition of employment. The User's failure to comply subjects the User to disciplinary action up to and including dismissal. In addition, the State reserves the right to seek any remedy available at law or in equity for any violation of this Agreement. Further, the User may be subject to civil and criminal penalties for harm, including financial harm, resulting from the

unauthorized use, disclosure, or deliberate unauthorized access of confidential information in violation of this agreement.

m. The User is bound by this Agreement indefinitely, and must protect the State's confidential information even after employment by any organization of the State ends.

n. Signing this Agreement does not guarantee the continuation of the employment relationship between the State and the User. This Agreement neither creates nor guarantees any additional rights or remedies on behalf of the User.

q. Any delay or failure to enforce any obligations, rights, or remedies under this Agreement, shall not constitute a waiver of such obligations, rights, or remedies created by the Agreement. This Agreement may be updated from time to time and should be accordingly renewed by the User upon request by the State. Such renewal shall serve only as an acknowledgement by this User of his or her awareness of the ongoing nature of this Agreement. Delay or failure to renew this Agreement does not negate the enforceability of any agreement regarding the subject matter of this Agreement previously entered into or acknowledged by the User.

My signature certifies that I understand and will abide by the statements contained in this document.

Printed Name: _____

Signature: _____

Date: _____