Personally Identifiable Information Breach Policy

Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. For the purposes of this policy there are three specified categories of PII: Public PII, Non-PII, and PII.

- **Public PII** – Some information, while may be considered PII (including, but not limited to, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials) are able to be found in public sources such as telephone books, public web site, and university listing.

- **Non-PII** – Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

- **PII** – For purposes of this policy, PII is any information about an individual maintained by Henrico CASA including, but not limited to, any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, or any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Henrico CASA will only collect PII when a specific purpose exists for its collection, such as information required for background clearances. PII will only be used for the purpose for which it was collected and only by the staff member responsible for using PII for that purpose. All records containing PII will be securely stored.

Approved: 10/14/2021

A “breach” of PII for purposes of this policy is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for any other than the authorized purpose.

Steps to be taken in the event of an actual or imminent breach:

1. Any employee who discovers an actual or imminent breach or has reason to believe that one may occur must immediately report the incident to the Executive Director or, if the Executive Director is unavailable, to the Board Chair through a phone call or SMS text message, regardless of the time or day of the week.

2. The Executive Director or designated member of the Board shall report an actual or imminent breach to DCJS no later than 24 hours after being informed of an occurrence of an actual breach or the detection of an imminent breach.

3. Henrico CASA will take prompt measures to: i) contain the incident, ii) initiate an investigation to determine whether a breach has occurred, iii) determine the scope of the breach and its origins, and iv) take countermeasures to mitigate the risk of harm to potentially affected individuals or to protect PII on behalf of the agency, including operating call centers and providing resources for potentially affected individuals.

I acknowledge that I have received a written copy of the Personally Identifiable Information Breach Policy, that I fully understand the terms of this policy, that I agree to abide by these terms, and that I am willing to accept the consequences of failing to follow the policy.

_____ _____

Staff/Volunteer Signature Date

_____ _____

Staff/Volunteer Name (printed) Date

Approved: 10/14/2021