Personally Identifiable Information (PII)
ExeVision Policy

1. Purpose: The policy describes ExeVision's procedures for properly handling PII and the consequences and corrective actions that will be taken when a breach has occurred.

2. Background: ExeVision applications collect data from vendors, contractors, and their employees. These data may include Personal Identifiable Information (PII) that may be used to distinguish or trace an individual's identity (NIST Special Publication 800-122). Consequently, ExeVision has established policies to protect the PII that is stored in the application databases.

3. Applicability: This policy applies to all ExeVision employees, contractors, subcontractors and those whose responsibility it is to manage information technology systems that contain PII. In particular, details of this policy are directed towards ExeVision developers, database administrators, and project managers but no Employee or Contractor is excluded from the provisions of this policy.

4. Personally Identifiable Information (PII): Personally identifiable information is data about a person that contains some unique identifier, including but not limited to name or Social Security Number, from which the identity of the person can be determined.

5. Protecting Personally Identifiable Information:

    a. Only the minimal amount of PII necessary to meet Agency business requirements is stored in the iPD database. Ensure that information that may be available in other sources available to the customer, may not be used to meet the business requirements.

    b. SSN (or FEIN) shall be visible only on web screens. SSN (FEIN) shall not be available as ad hoc reporting elements. This policy exists to prevent even authorized end-users from printing reports containing SSN(FEIN), names, addresses, birthdates from the database.

    c. PII shall only be stored in the iPD database where access is managed with user ID/password controls. Only developers and database administrators shall have access to the iPD database containing PII.
        i. Developer access to any database containing PII shall be restricted to fixing bugs associated with applications that access that database.

ii. Database administrators shall not run ad hoc queries that retrieve any production data, including PII, unless authorized as stated below.
iii. Database administrators shall make no copies of PII to be stored on their laptop, portable hard-drives, or paper.
iv. Exceptions to the policy restricting access to PII for developers and database administrators must be approved by senior ExeVision management.

d. Employees and Contractors shall not maintain PII on local development databases.
    i. When debugging an application problem that REQUIRES access to PII, a developer must:
        1. Obtain approval from ExeVision senior management to temporarily create a secure database on their local development database.
        2. Create a database extract containing PII to populate the development database. Whenever possible, only a subset database records will be used for the development database.
        3. Erase the development database within five (5) business days following completion of the bug fix.

e. If PII is sent over the internet, it must be transmitted using secure encryption methods (e.g. HTTPS protocol).

6. Information Data Breach**:** A data breach occurs when PII is viewed, leaked, or accessed by anyone who is not authorized to have access to this information. ExeVision employees and contractors are required to inform ExeVision management within two (2) hours of discovery of such breach. ExeVision senior management shall immediately begin an investigation of the extent of the data breach and contact the agency management within 24-hours of the initial report.

7. Corrective Action, Consequence and Penalties:

a. Employees**.** Individuals who do not comply with this policy may be subject to immediate termination. Compliance is mandatory. Employees shall review the PII policy within 5 days of beginning work at ExeVision.
b. Contractors**.** Breach of the ExeVision PII policy will be considered a breach of contract terms and contracts may be immediately cancelled. Contractors shall review the PII policy as part of contract award.