

## SP 13 – Security of Personally Identifiable Information (PII)

**Policy:** This policy provides guidance to help ADWS employees distinguish between sensitive and non-sensitive PII and determine which PII may be transmitted electronically. The ADWS policy is that if sensitive PII must be electronically transmitted, then it shall not be sent unless it is specifically protected by secure methodologies and in accordance with ADWS policies for Encryption, Information Classification, and Protection (SP 3).

ADWS policies for Encryption (SP 3.10) provide the standard to which encryption methodologies must conform.

This policy applies to ADWS employees, contractors, interns, guest researchers, and others who are authorized to use ADWS resources.

**Commentary:** With the increased use of computers for the processing and dissemination of data, the protection of PII has become more important to maintain public trust and confidence in an organization, to protect the reputation of an organization, and to protect against legal liability for an organization.

The term personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Examples include direct references such as name, address, social security number, and e-mail address. PII also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.

### Responsibilities

All covered personnel who utilize State of AR IT resources are responsible for adhering to this policy and any local Security of Personally Identifiable Information (PII)

<b>Role</b>	<b>Definition</b>
<b>Agency Management</b>	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for documenting, disseminating, and implementing the personnel security protection program throughout the agencies.
<b>Agency Security Liaison</b>	The Agency Security liaison are responsible for ensuring that personnel security risks are managed in compliance with the State's requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate personnel security controls required for personnel security protection.
<b>Human Resources</b>	The Human Resources (HR) ensures that human resource policies and procedures are developed to satisfy the appropriate personnel security controls for the state.
<b>Third Parties</b>	Third party service providers are responsible for managing third party personnel in accordance with this policy.

## **PII Classification**

### **Sensitive PII**

Sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a government newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother's maiden name, but each of these elements would not be sensitive independent of one another.

For the purpose of determining which PII may be electronically transmitted, the following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed in transmitting this data when associated with an individual:

- Place of birth
- Date of birth
- Mother's maiden name
- Driver's license number
- Biometric information
- Medical information, except brief references to absences from work
- Personal financial information
- Credit card or purchase card account numbers
- Passport numbers
- Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and result of background investigations
- Criminal history
- Any information that may stigmatize or adversely affect an individual.

This list is not exhaustive, and other data may be sensitive depending on specific circumstances.

Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed.

### **Non-sensitive PII**

The following additional types of PII may be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.

- Work phone numbers
- Work addresses
- Work and personal e-mail addresses
- Resumes that do not include an SSN or where the SSN is redacted

- General background information about individuals found in resumes and biographies
- Position descriptions and performance plans without ratings

However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

The determination that certain PII is non-sensitive does not mean that it is publicly releasable. The determination to publicly release any information can only be made by the official authorized to make such determinations. The electronic transmission of non-sensitive PII is equivalent to transmitting the same information by the U.S. mail, a private delivery service, courier, facsimile, or voice. Although each of these methods has vulnerabilities, the transmitted information can only be compromised as a result of theft, fraud, or other illegal activity.

**Examples of electronic transmission of PII, include, but are not limited to:**

- E-mail, text, and instant messages
- Document (s) attached to an e-mail message
- File Transfer Protocol (FTP)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- General Web Services
- File Sharing Services
- Electronic Data Interchange (EDI)

**Transmission of PII**

There are several methods operating units can use to transmit sensitive PII. These include:

Installing encryption software on a select number of desktops and designating those computers for the transmission of sensitive PII. The encryption methodology that is installed must conform to the standard for cryptographic-based security systems in accordance with ADWS policies on encryption (SP 3.10).

Using encryption software to encrypt the sensitive PII before sending it electronically, e.g., as an e-mail attachment. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

Using an application designed to protect the transmission of sensitive PII, e.g., Web-based applications that use TLS1.0, secure file share, or secure file transfer applications such as Secure Shell File Transport Protocol (SFTP).

**Questions regarding which PII**

If there is any question concerning the sensitive or non-sensitive nature of the PII, they should contact their supervisor who should consult the ADWS Information Security Officer.

**Standard:** Any information considered PII shall be treated as "confidential" in accordance with ADWS Information Security Policies on information classification and protection.

**Procedures:** Sanctions for misuse of PII shall be imposed in accordance with Information Security Policies and the Agency's Disciplinary Rules and Procedures Handbook.

### Annual Review

This policy, as well as all data classifications, must be reviewed at a minimum of every year or when there is a significant change that may impact the security posture of the data and/or system requiring a re-evaluation. A significant change includes but is not limited to data aggregation/commingling or decoupling of data. A reevaluation may also occur when a system classified as low or medium risk is later interconnected with a system classified as high risk.

### Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Version Number	Purpose/Change	Author	Date
1.0	Initial draft – to line manager	Paul Farris, Chief Security Officer	01/31/2023
2.0	Consultation draft – to working group	Paul Farris, Chief Security Officer	05/17/2023
2.1	Second consultation draft – to working group	Paul Farris, Chief Security Officer	09/19/2023
3.0	Final version – approved by MP	Paul Farris, Chief Security Officer	02/14/2024