A white logo with a blue flag on top of a building

Description automatically generated

Template

StateRAMP System Security Plan (SSP)

Service Provider Name

Information System Name

**VERSION:**

X.X

**DATE:**

YYYYMMDD

SYSTEM SECURITY PLAN

Prepared by:

|  |  |  |
| --- | --- | --- |
| Identification of Organization that Prepared this Document | | |
| A white square with a blue border  Description automatically generated | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Prepared for:

|  |  |  |
| --- | --- | --- |
| Identification of Cloud Service Provider | | |
| A white square with a blue border  Description automatically generated | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Template Revision History

| Date | Description |
| --- | --- |
| 3/31/2021 | Original publication |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version of SSP | Author |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

How to contact us

For questions about StateRAMP, or for technical questions about this document including how to use it, contact pmo@stateRAMP.org

For more information about the StateRAMP project, see www.stateRAMP.org.

Table of Contents

[1.1 Prospective PII Use 1](#_Toc162354813)

[1.2 Sources of PII and Purpose 1](#_Toc162354814)

[1.3 Access to PII and Sharing 1](#_Toc162354815)

[1.4 PII Safeguards and Liabilities 2](#_Toc162354816)

[1.5 Contracts, Agreements, and Ownership 3](#_Toc162354817)

[1.6 Accuracy of the PII and Redress 4](#_Toc162354818)

[1.7 Maintenance and Administrative Controls 4](#_Toc162354819)

[1.8 Business Processes and Technology 5](#_Toc162354820)

[1.9 Privacy Policy 5](#_Toc162354821)

## Prospective PII Use

Respond to the following questions:

|  |  |  |
| --- | --- | --- |
| 1. Are there any data fields in the platform or application that have been targeted for the collection or storage of PII? If yes, please name those fields. (SE-1, DM-1, IP-1) | | |
| *Click here to enter explanation.* | | |
| 1. If PII fields are used, can individuals “opt-out” of PII fields by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? (IP-1) | | |
| *Click here to enter explanation.* | | |
|  | Yes | Explain the circumstances of being able to opt-out of PII fields (either for specific data elements or specific uses of the data). (IP-1) |
|  |  | *Click here to enter explanation.* |
|  | No | It is not possible to opt-out. |

## Sources of PII and Purpose

1. Does CSP Name have knowledge of existing federal agencies that provide PII that gets imported into the system? (AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Has any agency that is known to provide PII to the system provided a stated purpose for populating the system with PII? (AP-1, AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Does CSP Name currently populate the system with PII? If yes, where does the PII come from and what is the purpose? (AP-1, AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Will any third party sources be providing PII that will be imported into the system (if known)? Please explain. (AP-1, AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

## Access to PII and Sharing

1. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared? (AP-1, AP-2, AR-8, IP-1, UL-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. What CSP Name personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP Name personnel to have access to the PII. (AR-8, UL-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. For CSP support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval? (IP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII. (UL-2)

|  |
| --- |
| *Click here to enter explanation.* |

## PII Safeguards and Liabilities

1. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access? (AR-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? (AR-1, AR-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Does the CSP Name provide annual security training include privacy training? Does CSP Name require their contractors that have access to the PII to take the training? (AR-5)

|  |
| --- |
| *Click here to enter explanation.* |

1. Who is privacy officer responsible for assuring safeguards for the PII? (AR-1)

|  |
| --- |
| *Click here to enter explanation.* |

1. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? (AR-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the PII owner advised about what federal agencies or other organizations share or have access to the data? (AR-1)

|  |
| --- |
| *Click here to enter explanation.* |

## Contracts, Agreements, and Ownership

1. NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this accountability described in contracts with customers? Why or why not? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do contracts with customers establish who has ownership rights over data including PII? (AR-2, AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do contracts with customers require that customers notify CSP Name if the customer intends to populate the service platform with PII? Why or why not? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do CSP Name contracts with customers establish record retention responsibilities for both the customer and CSP Name? (AR-2, AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the degree to which CSP Name will accept liability for exposure of PII clearly defined in agreements with customers? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

## Accuracy of the PII and Redress

1. Is the PII collected verified for accuracy? Why or why not? (DI-1)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the PII current? How is this determined? (DI-1)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?

*Click here to enter explanation.*

## Maintenance and Administrative Controls

1. If the system is operated in more than one site, how is consistent use of the PII maintained in all sites? Are the same controls used?

|  |
| --- |
| *Click here to enter explanation.* |

1. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? (AR-2, AR-3, DM-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? (AR-2, DM-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the system using new technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

|  |
| --- |
| *Click here to enter explanation.* |

1. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

|  |
| --- |
| *Click here to enter explanation.* |

1. Is access to the PII being monitored, tracked, or recorded? (AR-4)

|  |
| --- |
| *Click here to enter explanation.* |

1. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? (TR-2)

|  |
| --- |
| *Click here to enter explanation.* |

## Business Processes and Technology

1. Have the talking points found herein resulted in circumstances that requires changes to business processes?

|  |
| --- |
| *Click here to enter explanation.* |

1. Does the outcome of these talking points require that technology or operational changes be made to the system?

|  |
| --- |
| *Click here to enter explanation.* |

## Privacy Policy

1. Is there a system privacy policy and is it provided to all individuals whose PII you collect, maintain or store? (IP-1, TR-1, TR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the privacy policy publicly viewable? If yes, provide the URL. (TR-1, TR-3)

|  |
| --- |
| *Click here to enter explanation.* |