**DIGITAL IDENTITY RISK ACCEPTANCE STATEMENT**

This form is to be used to justify a risk acceptance of a known deficiency. The system/project manager is responsible for writing the justification and the compensating control. It is a requirement that a compensating control be defined in order to obtain full approval for a risk acceptance.

**Assessed Assurance Level (check all that apply):**

|  |  |  |
| --- | --- | --- |
| * IAL 1 | * AAL 1 | * FAL 1 |
| * IAL 2 | * AAL 2 | * FAL 2 |
| * IAL 3 | * AAL 3 | * FAL 3 |

**Implemented Assurance Level (check all that apply):**

|  |  |  |
| --- | --- | --- |
| * IAL 1 | * AAL 1 | * FAL 1 |
| * IAL 2 | * AAL 2 | * FAL 2 |
| * IAL 3 | * AAL 3 | * FAL 3 |

**If an Implemented Assurance Level differs from the Assessed Assurance Level, provide rationale:**

**If not accepting federated identities, provide rationale:**

**If an Implemented Assurance Level differs from the Assessed Assurance Level, provide the following information:**

1. Risk Statement: Describe the Condition(s)/Scenario(s)/Event(s) that pose a risk to the system, and a description of the possible loss or incident that may occur.
2. Risk Impact Level: Low, Moderate, or High.
3. Impact Statement: Describe the impact to the overall Business Mission, Assets, and/or Individuals as a result of not implementing the Assessed Assurance Level.

I certify that compensating controls will be implemented in the absence of the controls recommended by the assessor. I also certify that the compensating controls will provide a level of security and protection equivalent to the capability or level of security and protection that is needed for the information system.

* **Yes**. I certify that compensating controls will be implemented in the absence of the controls recommended by the assessor, at an appropriate level of security and protection.
* **No**. I have a waiver stating compensating controls are not required. (If a waiver is required, attach a copy.)
* **No**. I do not certify that compensating controls will be implemented in the absence of the controls recommended by the assessor, at an appropriate level of security and protection, and I do not have a waiver.
  + Justification for this decision:

System/Business Owner Name (printed): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

System/Business Owner Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Approval and Conditions:**

I hereby acknowledge that I have reviewed the aforementioned request for a Risk Acceptance decision, and certify that:

* **Yes**. I understand and accept responsibility for the outstanding risk related to the deployment and use of this application or service for the requested scope and timeframe.

<Insert reason for acceptance such as: I find the compensating controls are adequate, or the risk to the organization’s mission is acceptable; therefore, additional controls need not be applied.>

* **Yes, for a temporary period while controls are improved.** I accept responsibility for the outstanding risks related to the deployment/use of this application or service; however, I find the current level of control inadequate. The following controls must be implemented by **<date>**:

<List the scope and timing constraints and/or controls that need to be implemented.>

* **No.** I find the residual risk greater than the potential business benefit. This risk acceptance request is denied. The System Owner is to provide an action plan to mitigate this risk no later than **<Provide date>**.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizing Official or Designated Representative Name (Printed)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizing Official or Designated Representative Signature Date

**As applicable:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ISSO or Risk Functional Manager Name (Printed)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ISSO or Risk Functional Manager Signature Date

Acceptance by the Agency Chief Information Security Officer (CISO), Senior Agency Official for Privacy (SAOP), and the Agency Chief Information Officer (CIO) is needed for a risk that is categorized as a HIGH risk OR a risk that is associated with an Agency Enterprise System.

* **No.** This risk acceptance does not require concurrence by the Agency CISO, Agency SAOP, and the Agency CIO.
* **Yes**. This risk acceptance requires concurrence by the Agency CISO, Agency SAOP, and the Agency CIO.
* **Yes**. I/we approve this Risk Acceptance.
* **No**. I/we do not approve this Risk Acceptance. See attached decision document.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agency Chief Information Security Officer Name (Printed)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agency Chief Information Security Officer Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Senior Agency Official for Privacy Name (Printed)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Senior Agency Official for Privacy Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agency Chief Information Officer Name (Printed)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agency Chief Information Officer Signature Date