**Information Asset Identification Worksheet**

**Completed By:** Dustin Crewell

**Completed Date:** 6/27/2022

**Name of Information Asset:** RRSM Rent System

**Information Asset Description/Comment:**

**Information Asset Use:**

**Information Asset Format:**
(i.e., paper, electronic)

**Information Asset Storage:**
(e.g., file cabinet, safe, database, network share, CD/DVD, portable drive)

**Source of Information:**

**Business Process(es) Supported:**

**Information Owner:** Woody Pascal

**Information Custodian:**

**Internal Information User(s):**

**External Information User(s):**
(e.g., other State Agencies, other government agencies, public)

**Information Asset ID Number:**

# Information Classification Worksheet

## Confidentiality Questions

| | No | Yes |
|---|---|---|
| 1) Is the information publicly available? | X | |

| | No | Yes |
|---|---|---|
| 2) Does the information include or contain PPSI (Personal, Private or Sensitive Information)? | | |

**Please note that many of the questions overlap across Information Classification and Digital Identity. While the intent of the questions may be different, please consider the system's digital identity ratings (if available) when filling out this worksheet.**

| | 0-None | 1-Limited Impact | 2-Serious Impact | 3-Severe Impact |
|---|---|---|---|---|
| 3) What **impact** does unauthorized disclosure of information have on **health and personal safety?** | X | | | |
| 4) What is the **financial or agency liability impact** of unauthorized disclosure of information? | | X | | |
| 5) What **impact** does unauthorized access of sensitive information have the **state entity mission**? | X | | | |
| 6) What **impact** does unauthorized disclosure of information have on the **public trust, agency reputation, and public interests**? | | | X | |
| 7) Is confidentiality **mandated by law or regulation**? If yes, what is the **impact** of unauthorized disclosure of information. If no, do not make a selection. | | | X | |
| 8) Is the information intended for **limited distribution**? If yes, what is the **impact** of unauthorized disclosure. If no, do not make a selection. | | | X | |

| | |
|---|---|
| Overall: | Moderate |

## Integrity Questions

| | No | Yes |
|---|---|---|
| 1) Does the information include medical records? | X | |
| 2) Is the information (e.g. security logs) relied upon to make critical security decisions? | X | |

| | 0-None | 1-Limited Impact | 2-Serious Impact | 3-Severe Impact |
|---|---|---|---|---|
| 3) What **impact** does unauthorized modification or destruction of information have on **health and safety**? | X | | | |
| 4) What is the **financial impact** of unauthorized modification or destruction of information? | | | X | |
| 5) What **impact** does unauthorized modification or destruction of Information have on the **state entity mission**? | | | X | |
| 6) What **impact** does unauthorized modification or destruction of information have on the **public trust**? | | | X | |
| 7) Is integrity **addressed by law or regulation**? If yes, what is the **impact** of unauthorized modification or destruction of information. If no, do not make a selection. | | | X | |

# Information Classification Worksheet

| | | | | |
|---|---|---|---|---|
| 8) Is the information (e.g. financial transactions, performance appraisals) **relied upon to make business decisions**? If yes, what is the **impact** of unauthorized modification or destruction of information. If no, do not make a selection. | | | 2 | |
| | Overall: | Moderate | | |

## Availability Questions

| | As Time Permits | Within 1 to 7 Days | 24 hrs per day / 7 days per week |
|---|---|---|---|
| 1) This information needs to be **provided** or **available:** | | X | |

| | 0-None | 1-Limited Impact | 2-Serious Impact | 3-Severe Impact |
|---|---|---|---|---|
| 2) What is the **impact to health and safety** if information were **not available** when needed? | | X | | |
| 3) What is the **financial impact** if information were **not available** when needed? | | X | | |
| 4) What is the **impact to the State Entity mission** if information were **not available** when needed? | | | X | |
| 5) What is the **impact to the public trust** if the information were **not available** when needed? | | | X | |
| Overall: | Moderate | | | |

**Information Owner** - Print

**Date**

**Information Owner** - Signature

# Information Classification Worksheet

**ISO/Designated Security Representative** - Print

**Date**

**ISO/Designated Security Representative** - Signature

# Digital Identity Assessment Worksheet

## Identity Assurance Level Assessment

| | No | Yes |
|---|---|---|
| 1) To provide the service, do you need any personal information?<br>**If no, IAL1. Identity assurance level assessment is complete.** | | X |

| | No | Yes, or I don't know |
|---|---|---|
| 2) To complete the transaction, do you need the information to be validated?<br>**If no, IAL 1. Identity assurance level assessment is complete.** | | X |

**Please note that many of the questions overlap across Information Classification and Digital Identity. While the intent of the questions may be different, please consider the system's information classification when filling out this worksheet.**

** This section defines the potential impacts for each category of harm. Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) SHALL be evaluated separately.*

| 3) What are the risks (to the organization or the subject) of providing the digital service? | | N/A | Low | Moderate | High |
|---|---|---|---|---|---|
| Consider in the context of identity proofing.<br><br>Proofing errors with potentially worse consequences require higher levels of assurance. | Inconvenience, distress, or damage to the standing or reputation | | X | | |
| | Financial loss or agency liability | | X | | |
| | Harm to agency programs or public interests | | X | | |
| | Unauthorized release of sensitive information | | | X | |
| | Personal Safety | | X | | |
| | Civil or criminal violations | | X | | |
| | Overall: | IAL2 | | | |

If the above is assessed at **IAL 2**, AND you **do not need to resolve an identity uniquely**, AND you **can accept references** THEN **use references if you can** complete the transaction or offer the service without complete attribute values.

## Authenticator Assurance Level Assessment

** This section defines the potential impacts for each category of harm. Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) SHALL be evaluated separately.*

| 1) What are the risks (to the organization or the subject) of providing the digital services? | | N/A | Low | Moderate | High |
|---|---|---|---|---|---|
| Consider in the context of authentication.<br><br>Authentication errors with potentially worse consequences require higher levels of assurance. | Inconvenience, distress, or damage to the standing or reputation | | X | | |
| | Financial loss or agency liability | | X | | |
| | Harm to agency programs or public interests | | X | | |
| | Unauthorized release of sensitive information | | | X | |
| | Personal Safety | | X | | |
| | Civil or criminal violations | | X | | |

| | No | Yes |
|---|---|---|
| 2) Are you making personal data accessible? | | X |
| Overall: | AAL2 | |

## Federation Assurance Level Assessment

| | No | Yes |
|---|---|---|
| 1) Are you federating?<br>**If no, FAL is not applicable. Assessment is complete.** | X | |

** This section defines the potential impacts for each category of harm. Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) SHALL be evaluated separately.*

| 2) What are the risks (to the organization or the subject) of providing the digital services? | | N/A | Low | Moderate | High |
|---|---|---|---|---|---|
| Consider in the context of federation.<br><br>Federation errors with potentially worse consequences require higher levels of assurance. | Inconvenience, distress, or damage to the standing or reputation | | | | |
| | Financial loss or agency liability | | | | |
| | Harm to agency programs or public interests | | | | |
| | Unauthorized release of sensitive information | | | | |
| | Personal Safety | | | | |
| | Civil or criminal violations | | | | |

| | No | Yes |
|---|---|---|

# Digital Identity Assessment Worksheet

| | | | |
|---|---|---|---|
| 3) Will personal data be in the assertion? | | | |
| | | **No** | **Yes** |
| 4) Are you using front channel assertion presentation? | | | |
| | Overall: | N/A | |

**Information Owner** - Print

**Date**

**Information Owner** - Signature

**ISO/Designated Security Representative** - Print

**Date**

**ISO/Designated Security Representative** - Signature

## Compliance and Data Type Indicators

| Compliance Indicators | Yes | No | Description | Other Information |
|---|---|---|---|---|
| 42 CFR Part 2 Indicator | | X | Confidentiality of Alcohol and Drug Abuse Patient Records | |
| CJIS | | X | Criminal Justice Information Services | |
| DPPA | | X | Driver's Privacy Protection Act of 1994 | |
| FERPA | | X | Family Educational Rights and Privacy Act | |
| FISMA | | X | Federal Information Security Management Act | |
| FTA | | X | Federal Transit Administration | |
| GLBA | | X | Gramm-Leach Bliley Act | |
| HIPAA | | X | Health Information Portability and Accountability Act | May govern PHI |
| MARS-E | | X | Minimum Acceptable Risk Standards for Exchanges | Applied to Health Exchanges |
| Mental Hygiene | | X | Mental Hygiene Law of NYS | |
| MUSL | | X | Multi-State Lottery Association | |
| PCI | | X | Payment Card Industry Data Security Standard | |
| Pub1075 | | X | IRS Publication 1075 | Governs FTI |
| HIV/STD | | X | HIV virus attacking immune system | |
| SSA | | X | Social Security Administration | Governs a specific form of PII/PPSI involving SSN and associated data from SSA |

| Data Type Indicators | Yes | No | Description | Other Information |
|---|---|---|---|---|
| PII | X | | Personally Identifiable Information | |
| PHI | | X | Personal Health Information | |
| [Add Other Data Types as Needed] | | | | |
| | | | | |
| | | | | |

NYS ITS Policies and Standards recommend that controls be implemented for these data type:
https://its.ny.gov/document/information-security-controls-standard

NYS Information Security Breach and Notification Act
The NYS Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law. Copies of these sections can be found on the New York State Legislature Site.

State entities and persons or businesses conducting business in New York who own or license computerized data which includes private information must disclose any breach of the data to New York residents (state entities are also required to notify non-residents, see Information Security Policy NYS-P03-002.)

Breach Notification
https://its.ny.gov/eiso/breach-notification