# Standard: *Indiana Privacy Program Data Classifications*

Version: 1.1 (7/2023)

**AUTOMATED DECISIONMAKING**

- Does the source system leverage artificial intelligence (AI) and/or machine learning (ML) to process data?
    - y/n

**GRANULARITY CLASSIFICATION**

- Tier 1 – Row-level identified
- Tier 2 – Row-level de-identified
- Tier 3 – Aggregate, not suppressed
- Tier 4 – Aggregate, suppressed

**PRIVACY IMPACT RISK CLASSIFICATION**
(SOURCE: *State of Indiana Privacy Impact Assessment Methodology: A NIST-Based Framework to Support Enhanced Privacy Protections within Government*)

- High
    - The potential impact is HIGH if the privacy risk could be expected to have severe adverse effects. Severe adverse effects of a privacy risk means that there could be: (i) numerous legal implications due to the risk; (ii) severe disruptions to the agency or division's operations where they are unable to perform their primary functions, or the effectiveness of the functions are severely reduced; and (iii) severe implications on the public's perception of and trust in the agency or division.
- Moderate
    - The potential impact is MODERATE if the privacy risk could be expected to have significant adverse effects. Significant adverse effects of a privacy risk means that there could be: (i) possible legal implications due to the risk; (ii) disruptions to the agency or division's operations where they are able to perform their primary functions, but the effectiveness of the functions are significantly reduced; and (iii) possible implications on the public's perception of and trust in the agency or division.
- Low
    - The potential impact is LOW if the privacy risk could be expected to have limited adverse effects. Limited adverse effects of a privacy risk means that there could be: (i) no legal implications due to the risk; (ii) limited implications on the business operations of the agency and divisions; and (iii) little to no impact on the public's perception of and trust in the agency or division.

**SECURITY RISK CLASSIFICATION**
(SOURCE: IOT Statewide IT Policy: *Data Classification and Categorization*)

- Confidential-Sensitive

    - Confidential-Sensitive data is data that the State is legally or contractually prevented from disclosing.
- Confidential-Proprietary
    - Confidential-Proprietary data includes information and records associated with the business and policy-decision making of the State, including (but not limited to) details of cybersecurity, vulnerability, risk mitigation, and/or information security plans, policies, and/or standards.
- Non-Confidential
    - Data that is not protected under the definition and examples of either Confidential-Sensitive or Confidential-Proprietary data above shall be classified as Non-Confidential. Data classified as Non-Confidential is not inherently open for public sharing or disclosure.
    - If Non-Confidential data is aggregated with data classified at the Confidential-Sensitive or Confidential-Proprietary level (e.g., in a shared database or system), the overall classification of the data should reflect the highest level of classification present in the aggregate.

**RECORDS RETENTION**

- Record Series Number: _____

**REGULATORY CLASSIFICATION**

- FIPA (Indiana Fair Information Practices Act)
    - (*Note, all personal information, as defined in IC 4-1-6-1(2), triggers FIPA applicability. In the case of information maintained by Indiana state agencies, it is likely that FIPA applies, in addition to other regulations.)
- HIPAA (Health insurance Portability & Accountability Act)
- SUD (Substance Use Disorder Patient Records)
- SNAP (Supplemental Nutrition Assistance Program)
- PCI (Payment Card Industry)
- FTI (Federal Tax Information)
- FERPA (Family Educational Rights and Privacy Act)
- FISMA (Federal Information Security Management Act)
- CJIS (Criminal Justice Information Services)
- CMS (Center for Medicare & Medicaid)
- SSA (Social Security Administration)
- DPPA (Drivers Privacy Protection Act)
- UC (Unemployment Compensation)
- Other

# Standard: *Indiana Privacy Program Data Classifications*

Version: 1.1 (7/2023)

**RELEASABILITY QUESTIONNAIRE**

- Is this dataset public?
  - y/n
- If 'no' was answered in the previous question, may it be made public?
  - y/n/unsure

**STORAGE LOCATION & TRUST**

- Is this information stored on-premises or in the cloud?
  - On-premises storage
  - Cloud storage
- If 'cloud storage' was answered in the previous question, are the State of Indiana Additional Terms and Conditions for Cloud Service Engagements (i.e. state cloud terms) incorporated into the contract with the vendor storing the information?
  - y/n