PRIVACY IMPACT ASSESSMENT POLICY

POLICY STATEMENT:

Increased connectivity of computers and databases makes more data available to individuals, businesses, and agencies. As a result, the potential for unauthorized disclosure, modification, or destruction of personal, financial, business, and other data also has increased. The department shall create privacy impact statement prior to the implementation of any information technology data system. Privacy impact statements consist of a Privacy Threshold Assessment (PTA), a Privacy Impact Assessment (PIA), or both.

AUTHORITY:

Ohio Revised Code (ORC) 125.18; ORC 149.011; ORC 149.434; ORC 1347

REFERENCES:

IT Bulletin ITB-2008.02, "Privacy Impact Assessments"

Ohio IT Policy ITP-B.11, “Data Classification”

Executive Order 2007-013S

Ohio IT Standard ITS-SEC-01, “Data Encryption and Cryptography”

SCOPE:

All Districts, Divisions, Offices, and Contractors at the Ohio Department of Transportation. Any personnel who won, manage, or maintain any ODOT-owned information systems that reference, use, or store sensitive data. Any electronic data records that are stored on or pass through ODOT’s systems.

BACKGROUND AND PURPOSE:

The most effective way to protect information and systems, in terms of both implementation and costs, is to incorporate privacy and security into the architecture of each. Adding privacy and security after initial development can be more costly and problematic. State agencies are required to create privacy impact statements in accordance with Section 125.18 of the Ohio Revised Code. Performing a Privacy Threshold Analysis (PTA) or a Privacy Impact Assessment (PIA) upon the collection of new types of information, or at the beginning of the development or acquisition of a new information system that maintains personally identifiable information, will help a state agency to determine most, if not all, of the necessary security controls.
A PIA shall address the following concerns:

- what information is collected by the information system;
- whether the information system contains personally identifiable information as defined in this bulletin;
- why the information is collected by the state agency;
- intended uses of the information;
- with whom the information will be shared, such as other agencies or contractors;
- what opportunities individuals have to decline to provide personally identifiable information or to consent to particular uses of their information, and how this consent is granted; how the information will be secured; the retention schedule for maintaining personally identifiable information; and methods for disclosure and destruction of personally identifiable information.

DEFINITIONS:

**Information Systems** – Any application, spreadsheet, database, data collection, or other electronic system that could contain sensitive information.

**Privacy Statement** – A privacy statement includes a PTA, a PIA, or both. A privacy statement indicates how any risks will be mitigated for the information system if it includes sensitive data.

**Privacy Threshold Assessment (PTA)** – Contains basic questions about the nature of the system in addition to a basic system description and can help a system owner or program manager efficiently make the determination of whether a PIA is required.

**Privacy Impact Assessment (PIA)** – An analysis of how information is collected, stored, protected, shared, and managed in an IT system or online collection.

**Electronic Data** – Electronic information stored or passed through ODOT’s systems. Any data kept on paper are not part of this policy.

**TRAINING**

The distribution of communication of this policy along with subsequent guidelines, standards, and standard procedures will constitute training for this policy.

**FISCAL ANALYSIS**

The required infrastructure for implementation of this policy is already budgeted for as part of IT infrastructure improvements. Therefore this policy does not have additional fiscal impact.