THE TEXAS STATE UNIVERSITY SYSTEM®

Artificial Intelligence (AI) Risk Management Policy

Artificial Intelligence (AI) Risk Management

Purpose: The purpose of this policy is to define information security controls concerning artificial intelligence risk management.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution's information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Management: This policy is managed by the TSUS Information Security Council and will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

POLICY/PROCEDURE

1. Policy Statements

1.1. Artificial Intelligence controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1. Texas State University System defines technical policy terms in the information technology glossary.

3. Procedures

Authority - TAC §219.21

3.1. Component institutions must:

3.1.1. Develop procedures to facilitate the implementation of the Artificial Intelligence Risk Management policy and associated controls;

3.1.2. Review and update AI risk management procedures at an institution-defined frequency; and

3.1.3. Designate an institution-defined AI Risk Officer as responsible for managing, developing, documenting, and disseminating institutional AI risk management procedures related to the controls in this policy.

4. AI Risk Officer Responsibilities
Authority – TAC §219.21

4.1. Each component AI Risk Officer is responsible for:

4.1.1. Promoting ethical AI system procurement, development, deployment, and use within their institution, consistent with the AI Code of Ethics established by TAC §219.11 and the AI Risk Management Framework published by the National Institute of Standards and Technology.

4.1.2. Developing a process to identify and inventory all implementations of AI systems that qualify as heightened scrutiny AI systems.

4.1.3. Ensuring that risk assessments of heightened scrutiny AI systems are completed, evaluated, and reviewed for consistency with the standards established in TAC §219.21 prior to deployment.

4.1.4. Authorizing or denying deployment of the system based on the risk and mitigation measures identified in the risk assessment.

4.1.5. Ensuring AI impact assessments of a heightened scrutiny AI system are completed, evaluated, and reviewed for consistency with the standards established in TAC §219.23 prior to deployment.

4.1.6. At minimum, notifying the component's institution head or their designee of a decision to deploy a heightened scrutiny AI system.

4.1.7. Maintaining a record of completed risk and impact assessments and all relevant documents for as long as required by the applicable state records retention schedule.

4.1.8. Establishing a process for receiving and responding to redress requests.

5. Risk Assessment for Heightened Scrutiny AI Systems
Authority – TAC §219.22

5.1. Prior to developing, procuring, deploying, or using a heightened scrutiny AI system, component institutions must:

5.1.1. Conduct a risk assessment to consider the probability and severity of harm that could occur as the result of implementation of the AI system.

5.2. The Risk assessment shall consider and document:

5.2.1. The AI system's known security risks and mitigation steps available to limit those risks;

5.2.2. The AI system's performance metrics relating to accuracy and operational efficiency; and

5.2.3. The AI system's transparency, including information about:

5.2.3.1.1. The AI system's algorithms and how the system makes decisions;

5.2.3.1.2. The data used to train the AI system's model; and

5.2.3.1.3. The availability of inputs and outputs to monitor the system's decision-making over time.

6. Impact Assessments for Heightened Scrutiny AI Systems

Authority – TAC §219.23

6.1. Component institutions that deploy or use a heightened scrutiny AI system must conduct, or have conducted by a vendor that contracts with the component institution for its deployment or use, an impact assessment of heightened scrutiny AI systems:

6.1.1. Prior to deploying the AI system; and

6.1.2. At the time any material change is made to:

6.1.2.1. The AI system

6.1.2.2. The state or local data used by the system; or

6.1.2.3. The intended use of the system.

6.1.3. If a vendor that contracts with a component institution conducts an impact assessment, the component must:

6.1.3.1. Receive a copy of the completed impact assessment and

6.1.3.2. Treat the vendor's copy as the document of record.

6.1.4. Component institutions shall make a copy of the impact assessment available to the Texas Department of Information Resources on request.

6.2. The impact assessment must include:

6.2.1. A description of the system, including its training data, model, and intended use;

6.2.2. How the component will use the system and who within the component is responsible for its deployment and ongoing monitoring and evaluation;

6.2.3. Whether the system will process or store any PII provided by the component or the users of the component's system and whether the system will use that information to train the model;

6.2.4. Potential risks of unlawful harm that the component identifies and steps the component can take to limit those risks;

6.2.5. System limitations identified by the component;

6.2.6. How the component will monitor the system outputs to evaluate accuracy and harm and identify the intervals at which the monitoring will occur; and

6.2.7. The retention duration for the system's inputs and outputs and the method for deleting outputs once the identified retention period has passed.

7. Guidelines for Frameworks, Policies, and Trainings for Heightened Scrutiny AI Systems

Authority – TAC §219.24

7.1. Component institutions must:

7.1.1. Adopt an acceptable use policy to prevent uses other than those approved by the component.

7.1.2. Adequately train all employees on the acceptable use policy.

7.1.3. Train employees or contractors who access, use, or manage the heightened scrutiny AI system regarding identified risks and appropriate methods for mitigating those risks.

7.2. Component institutions that contract with vendors to deploy a heightened scrutiny AI system shall contractually require those vendors to:

7.2.1. Implement an AI risk Management Framework such as that published by the National Institute of Standards and Technology or a comparable standard; and

7.2.2. Adopt the AI Code of Ethics found at TAC §219.11.

8. Human Oversight and Control

Authority – TAC §219.11(h)

8.1. Component institutions:

8.1.1. Must deploy AI systems in ways that enable humans to review and analyze inputs and outputs at appropriate intervals throughout the AI lifecycle.

8.1.2. May incorporate a level of human oversight reasonably commensurate to the risks associated with a particular AI system, with heightened scrutiny AI systems requiring increased human oversight relative to lower risk systems; and

8.1.3. Must ensure AI systems can be paused, restricted, or disabled until harmful or inaccurate decision making can be remedied.

9. Redress

Authority – TAC §219.11(f)

9.1. Component institutions must provide a mechanism to seek redress for those impacted when an AI system makes a consequential decision that results in unlawful harm impacting their rights or access to governmental services.

9.2. Component institutions must have a designated point of contact for individuals to address when seeking information about an unfair consequential decision; and

9.3. Must develop internal procedures to allow employees to identify and remedy negative impacts caused using AI systems.

10. Transparency

Authority – TAC §219.11(g)

10.1. Component institutions must disclose when individuals interact with:

10.1.1. A public-facing AI system;

10.1.2. When an AI system used to make consequential decisions impacting their rights or access to governmental services; and

10.1.3. Must never represent AI systems as human when interacting with the public.

11. AI Data Privacy

Authority – TAC §219.11(h)

11.1. Component institutions may collect and maintain only that PII needed for operations and must establish a process to delete PII consistent with records retention schedules and other legal requirements.

12. Issuance of Institutional Standards

Authority – TSUS

12.1. Component institutions must develop and maintain one or more institution-level standards regarding AI risk management covered by this policy. The standard(s) must include the following items to a non-confidential level of detail:

12.1.1. Component-level adoption of the AI Code of Ethics found at TAC §219.11.

12.1.2. Designation of an AI Risk Officer whose responsibilities include those identified in section four of this policy.

12.1.3. Procedures to implement risk and impact assessments in compliance with sections five and six of this policy.

12.1.4. Procedures to implement section seven of this policy.

12.1.5. Establish a review cycle for the component-level standard(s) on AI Risk Management.