



UNITED INDEPENDENT SCHOOL DISTRICT

AGENDA ACTION ITEM

TOPIC: Approval to designate Rene Cruz, Director of Information Technology,

As the Artificial Intelligence (AI) Risk Officer

SUBMITTED BY: Hector J Perez  **OF:** Technology Department

APPROVED FOR TRANSMITTAL TO SCHOOL BOARD: _____

DATE ASSIGNED FOR BOARD CONSIDERATION: September 16, 2026

RECOMMENDATION:

It is recommended that the UISD Board of Trustees discuss and take possible action to designate Rene Cruz, Director of Information Technology, as the District's AI Risk Officer as mandated by the Texas Department of Information Resources (DIR) under Texas Administrative Code Title 1, Chapter 219 (1 TAC Chapter 219), that requires school districts to formally adopt the state's AI code of ethics to govern ethical procurement, development, deployment, and use of artificial intelligence systems; and (1 TAC 219.21) which mandates that the district designates a qualified employee as the official AI Risk Office to oversee AI, promote ethical procurement, and manage required risk assessments.

RATIONALE:

Consider a Possible Action to Designate the District AI Risk Officer and Adopt the State AI Code of Ethics in Compliance with 1 TAC Chapter 219 and 1 TAC Chapter 219.21

BUDGETARY INFORMATION:

No Impact on Budget

POLICY REFERENCE & COMPLIANCE:

In accordance with Texas Administrative Code Title 1, Part 10, Chapter 219, Section 11 (1 TAC § 219.11(a)) and mandated by Texas Government Code § 2054.702.

DIR AI Code of Ethics

The requirement to adopt the State AI Code of Ethics is formally established under Texas Administrative Code Title 1, Part 10, Chapter 219, Section 11 (1 TAC § 219.11(a)) and mandated by Texas Government Code § 2054.702.

The Department of Information Resources (DIR) AI Code of Ethics consists of 10 distinct compliance pillars. These are detailed in your resources (specifically the *K-12 AI Guidance and Guardrails* workbook and the *AI Risk Officer's Guide*) as a comprehensive compliance checklist:

The 10 Pillars of the DIR AI Code of Ethics

1. Human Oversight and Control
 - Districts must deploy AI systems in ways that allow humans to review and analyze inputs and outputs at appropriate intervals.
 - The district must establish technical or operational protocols to immediately pause, restrict, or disable ("kill-switch") any AI system if harmful or inaccurate outputs are detected.
2. Fairness
 - AI systems must not infringe upon the legally protected rights and liberties of students or staff, nor result in unlawful harm.
 - Districts must establish clear data governance practices throughout the AI lifecycle to actively prevent bias and ensure equitable treatment.
3. Accuracy
 - Districts must establish formal processes to monitor the accuracy of AI systems both before deployment and throughout their lifecycle.
 - Staff must be trained to verify AI outcomes for accuracy before acting on them, and districts should use human feedback or retrieval-augmented generation (RAG) to improve accuracy where feasible.
4. Redress
 - Districts must provide a clear method for students, parents, or staff to seek redress or appeal when an AI system makes a consequential decision that results in unlawful harm or impacts access to services.
 - *Note:* Districts can choose to route these appeals through their existing grievance policies, such as FNG(LOCAL), DGBA(LOCAL), and GF(LOCAL).
5. Transparency

- Districts must collaborate with developers to understand how the AI model works, its capabilities, its limitations, and the data it was trained on.
- Districts must explicitly disclose when individuals are interacting with a public-facing AI system (such as a website chatbot) and when AI is used to make material/consequential decisions affecting student or staff rights.
- School systems are strictly prohibited from representing an AI system as a human.

6. Data Privacy

- Districts must practice data minimization, collecting and retaining only the minimum Personally Identifiable Information (PII) necessary for operational functions.
- PII must be deleted consistent with local records retention schedules.
- Employees must be trained on the serious risks of inputting sensitive or student PII into public, unauthorized AI tools.
- Prior parental consent is required for storing biometric data (such as voiceprints/faceprints) or using health/wellness chatbots.

7. Security

- AI systems must be continuously monitored, secured, and tested to prevent or mitigate cyberattacks (such as data poisoning, prompt injection, or model exfiltration).
- Districts must contractually require AI system providers to disclose any known vulnerabilities and their resolutions in a timely manner.

8. Accountability and Liability

- Employees must be trained to use AI tools effectively, safely, and ethically.
- Districts must ensure that all third-party vendors are contractually bound to these exact AI ethical principles.
- AI systems must fully comply with all other applicable state and federal legal obligations (e.g., FERPA, COPPA, CIPA).

9. Evaluation

- The district must establish a recurring method to evaluate deployed AI systems to ensure they continue to provide tangible, ongoing benefits to students and staff.
- These evaluations must be formally documented.

10. Documentation

- Districts must maintain detailed records of the data sources used to train or supplement the AI system.
- The district must document how any AI system is modified or updated throughout its lifecycle.