Ethics Policy and Guidelines for Use of Texas Workforce Commission Data and Artificial Intelligence

[July 21, 2026]

OGC AI Risk Office SharePoint Page

Table of Contents

Ethics Policy and Guidelines for Use of Texas Workforce Commission Data and Artificial Intelligence 4
1. Purpose and General Requirements 4
1.1. Purpose 4
1.2. Definitions 5
1.3. Compliance with Applicable Laws, Rules, Regulations, and TWC Policies 8
1.4. Training 9
1.5. Violations 10
1.5.1. Obligation to Report 10
1.5.2. Disciplinary Action 10
2. Ethical Use of TWC Data 10
2.1. Privacy and Confidentiality of TWC Data and TWC Information 11
2.2. Data Minimization 12
2.3. Incomplete or Inaccurate Data; Misinterpreting Data 12
2.4. Honesty and Integrity with TWC Data 13
2.5. Accountability 13
2.6. Transparency 14
3. Ethical Procurement, Development, Deployment, and Use of AI 14
3.1. Ethical Development and Deployment of AI 15
3.1.1. Human Oversight and Control 15
3.1.2. Monitoring AI Systems for Accuracy 16
3.1.3. Evaluation 16
3.1.4. Documentation 17
3.1.5. Security 17
3.1.6. Accountability and Liability in the Procurement and Deployment of AI Systems 17
3.2. Ethical Use of AI 18
3.2.1. Restrictions on the Use of AI Systems 18
3.2.1.1. Never Use or Put TWC Data or TWC Information into Public AI 18
3.2.1.2. Use Only TWC-Approved AI 18

3.2.1.3. Unapproved AI Tools in Approved Software 19
3.2.1.4. Data Restrictions with TWC-Approved AI 19
3.2.2. Human Review of AI Output Required 20
3.2.2.1. Review of AI Output for Accuracy 20
3.2.2.2. Human Review Required for Consequential Decisions 21
3.2.3. Employees Are Responsible for AI Use in TWC Work Product ... 22
3.2.4. Fairness 22
3.2.5. Redress 23
3.2.6. Transparency 23
3.2.7. Data Privacy 24
3.2.8. Accountability and Liability 24
3.2.9. Any Heightened Scrutiny AI System Must Follow AI Minimum Standards 25

Ethics Policy and Guidelines for Use of Texas Workforce Commission Data and Artificial Intelligence

1. Purpose and General Requirements

1.1. Purpose

The State of Texas and the Texas Workforce Commission (TWC) embrace the transformative potential of Artificial Intelligence (AI) to revolutionize how TWC serves its customers. In alignment with TWC's 2027-2031 Strategic Plan, the "Texas Way" means leading from the front. We embrace technological advancement, including the strategic use of AI, not to replace the human touch, but to enhance it. This policy outlines a framework for ethically using TWC Data (defined below) and developing, deploying, and using AI Systems (defined below) to enhance efficiency, improve decision-making, and unlock new solutions to better serve the public. TWC believes that responsible AI adoption will lead to more effective government services, better resource allocation, and ultimately, a higher quality of service delivery for the Texans who use our services and programs. By making our systems more efficient, our staff can improve the quality of our programs—spending less time on paperwork and more time on the people we serve.

Although the use of AI has tremendous potential, human oversight will always be necessary. AI is a tool to assist, not replace, professional judgment. As such, it is a fundamental expectation that all TWC employees maintain an acute awareness of AI’s inherent limitations (including AI’s potential lack of contextual understanding, common sense, or impartiality) and play an active role in ensuring that AI Systems operate ethically.

To ensure the responsible use of AI, this policy is built on several key components that create clear expectations for all TWC employees:

- **Upholding Data Integrity and Privacy:** TWC employees are required to protect TWC Data, ensure its accuracy, and practice data minimization.
- **Ensuring Human Oversight and Accountability:** This policy mandates that all AI Systems are subject to human control and that employees are accountable for both the data and the AI they use.

- **Using AI Securely and Responsibly:** TWC employees must use only TWC-approved AI tools, never input confidential TWC data into public AI, and critically review all AI-generated content—especially any AI output used in connection with Consequential Decisions (defined below)—for accuracy and alignment with applicable laws and TWC policies before use.
- **Maintaining Transparency and Fairness:** The policy requires that the use of AI is transparent and that its application is fair and provides avenues for redress.

By following the guidelines in this policy, TWC employees will be able to harness the transformative benefits of AI while safeguarding public trust and promoting fair and impartial service delivery for the people of Texas.

Information regarding this policy and applicable laws and rules governing TWC employees' use of AI, including a link to this policy, is available on the AI Risk Office SharePoint page. Additional information on ethics issues, including the broader *Texas Workforce Commission Ethics Policy*, is available to TWC employees on the TWC Ethics SharePoint page.

1.2. Definitions

As used in this policy, the terms below shall have the following meanings, unless the context clearly indicates otherwise:

AI System has the meaning set forth in Texas Government Code § 2054.003(1-a): a machine-based system that for explicit or implicit objectives infers from provided information a method to generate outputs, such as predictions, content, recommendations, or decisions, to influence a physical or virtual environment with varying levels of autonomy and adaptiveness after deployment.

Consequential Decision has the meaning set forth in Texas Government Code § 2054.003(2-b): a decision that has a material legal or similarly significant effect on the provision, denial, or conditions of a person's access to a government service.

Controlling Factor has the meaning set forth in Texas Government Code § 2054.003(2-c): a factor that is: (A) the Principal Basis for making a Consequential Decision; or (B) capable of altering the outcome of a Consequential Decision.

Heightened Scrutiny AI System has the meaning set forth in Texas Government Code § 2054.003(6-a): an AI System specifically intended to autonomously make, or be a Controlling Factor in making, a Consequential Decision. The term does not include an AI System intended to:

(A) perform a narrow procedural task;

(B) improve the result of a previously completed human activity;

(C) perform a preparatory task to an assessment relevant to a Consequential Decision; or

(D) detect decision-making patterns or deviations from previous decision-making patterns.

Information Resources has the meaning set forth in Texas Government Code § 2054.003(7): the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, as well as associated personnel, including consultants and contractors.

Information Resources Technologies has the meaning set forth in Texas Government Code § 2054.003(8): data processing and telecommunications hardware, software, services, supplies, personnel, facility resources, maintenance, and training.

Knowingly means the person knew or should have known.

PHI: Personal Health Information. The term PHI includes information about the diagnosis, treatment, or payment for physical or mental medical or health related conditions or services of an individual.

PII: Personal Identifying Information. The term PII has the meaning set forth in Texas Business & Commerce Code § 521.002(a)(1): information that, alone or in conjunction with other information, identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; and

(E) telecommunication access device as defined by Section 32.51, Penal Code.

Examples of PII include:

- names, addresses, telephone numbers, and place of work on a business card;
- names, addresses, and telephone numbers in a public directory;
- names, addresses, and telephone numbers of attendees at a conference; and
- lists of TWC employee or customer names.

Principal Basis has the meaning set forth in Texas Government Code § 2054.003(11): the use of an output produced by a Heightened Scrutiny AI System to make a decision without:

(A) human review, oversight, involvement, or intervention; or

(B) meaningful consideration by a human.

SPI: Sensitive Personal Information. The term SPI includes information that, alone or in combination with available information, can identify an individual and that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of SPI would include an individual's first name or first initial and last name in combination with any one or more of the following items:

- Unique identification numbers, such as Social Security Numbers (SSNs), driver's license numbers, and other government-issued identification numbers;
- Unique biometric data, including an individual’s fingerprint, voiceprint, and retina or iris image;
- Financial information, such as an account number or credit/debit card number in combination with any required security code, access code,

or password that would permit access to an individual's financial accounts; and

- PHI.

TWC Data means any TWC Information that contains qualitative or quantitative data elements or data computations, regardless of the form or medium, including any data that has been manipulated or converted into another format or incorporated in any manner into a third party's records, files, or data compilations.

TWC Information Means any information maintained by TWC, including TWC Data, regardless of the form or medium. TWC Information includes any TWC Information that has been manipulated or converted into another format or medium (such as handwritten or electronic notes) and that portion of any TWC Information that has been incorporated in any manner into a third party's records, files, or data compilations.

Unlawful Harm has the meaning set forth in Texas Government Code § 2054.701: any condition in which the use of an AI System results in a Consequential Decision that causes harm to an individual who is a member of a state or federally protected class in violation of law. The term does not include a developer's or deployer's offer, license, or use of a Heightened Scrutiny AI System for the sole purpose of testing the system before deployment to identify, mitigate, or otherwise ensure compliance with state and federal law.

Use (including all variants): When used in reference to data, all variants of the term "use" include creating, acquiring, managing, manipulating, sharing, using, or disposing of data.

1.3. Compliance with Applicable Laws, Rules, Regulations, and TWC Policies

This policy incorporates guidance from applicable laws, regulations, and rules in the Texas Administrative Code, including with respect to data and AI ethics, applicable provisions in Texas Government Code § 2054.702 (Artificial Intelligence System Code of Ethics), 1 Texas Administrative Code § 219.11 (Code of Ethics and Ethical Principles of Artificial Intelligence), and applicable TWC policies.

As government employees, TWC employees must adhere to the laws of the State of Texas, and must not subvert the interests of the State to pursue their own personal interests. Additionally, TWC employees should be mindful

of their roles as public servants and, as such, must perform their official duties in an honest, professional, and ethical manner befitting the State of Texas and TWC.

Recognizing the importance of integrity and accountability in public service, TWC employees must comply with all applicable laws, rules, regulations, and TWC policies in the use of TWC Data and the deployment and use of AI and avoid even the appearance of violating the law or this policy. Other applicable policies include:

- TWC Generative AI Guidelines,
- TWC Information Security Manual,
- TWC Privacy Manual,
- TWC Personnel Manual, and
- TWC Ethics Policy.

Relevant Division-level policies may also apply, and TWC employees must be aware of, and abide by, those policies as well.

Additionally, as a governmental body, TWC has an obligation under the Texas Public Information Act, chapter 552 of the Government Code (PIA), to provide public information that is responsive to open records requests (provided such information is not subject to an exception under the PIA). Accordingly, TWC employees should be mindful of this obligation and understand that certain TWC Data and TWC Information, including any information input to or generated from the use of data visualization tools or AI, could be subject to disclosure under the PIA. If a TWC employee receives a request for any TWC Information from a member of the public, the employee should refer the requestor to the Open Records Department (requestors may contact Open Records via the TWC Open Records web portal or by email at open.records@twc.texas.gov).

TWC employees are encouraged to reach out to the Office of General Counsel with any questions on potentially applicable laws and regulations.

1.4. Training

Each TWC employee must annually take and pass TWC's AI Awareness Training, which includes training on the information in this policy and the standards applicable to state employees' development, deployment, and use of AI.

1.5. Violations

1.5.1. Obligation to Report

TWC employees shall report any conduct or activity that violates this policy to TWC management and/or, as appropriate, the AI Risk Office (ai.riskoffice@twc.texas.gov), the Chief Ethics Officer, the Director of Fraud Deterrence and Compliance Management (FDCM), or the Privacy Officer. TWC employees may also report a violation of this policy by sending an email to the AI Risk office at ai.riskoffice@twc.texas.gov. Employees may also report a privacy or security event here.

TWC is required to report certain violations of this policy or applicable statutes and rules governing AI to the Department of Information Resources and the Office of the Attorney General.

1.5.2. Disciplinary Action

TWC employees who breach the obligations outlined in this policy may face disciplinary measures, up to and including termination from their position. Additionally, any TWC employee who violates this policy may also be subject to applicable civil or criminal penalties if the employee’s action or inaction also violates a statute or rule.

2. Ethical Use of TWC Data

TWC Data is a powerful asset that, when analyzed ethically and responsibly, can significantly enhance TWC's ability to serve the people of Texas. By harnessing the power of data analytics tools, TWC can gain valuable insights, improve decision-making, and develop more effective programs to support workforce development and economic opportunity. However, the use of TWC Data must be guided by ethical principles; otherwise, it can present risks to TWC's success. TWC employees should be mindful of these principles and understand their obligations to ensure the ethical use of TWC Data, preserve the privacy of TWC Data, and adhere to appropriate levels of transparency.

The ethical use of TWC Data focuses on the following core concepts:

- **Impact on people.** TWC Data represents characteristics of individuals and is used to make decisions that affect people’s lives. TWC employees must ensure the quality and reliability of TWC Data.

- **Potential for misuse.** Misusing TWC Data can negatively affect people and organizations. Accordingly, TWC employees must constantly be on guard to prevent unauthorized access to and use of TWC Data.

- **Economic value.** TWC Data has an economic value. Thus, TWC employees must determine how that value may be accessed and by whom, while always prioritizing ethical and responsible use.

2.1. Privacy and Confidentiality of TWC Data and TWC Information

Although similar concepts, privacy and confidentiality have distinct meanings. ***Privacy*** means protecting individuals' rights to be free from unwarranted intrusion into their private lives, and ***confidentiality*** means protecting information from unauthorized access, disclosure, or use. TWC employees should always be vigilant about protecting the privacy and confidentiality of TWC Data and TWC Information, particularly with respect to PII, SPI, and PHI. Access to confidential TWC Information (including PII, SPI, and PHI) is authorized only if the access is required to meet TWC program needs, is needed for purposes specifically listed in a TWC contract, or is otherwise authorized by law.

Accordingly, all TWC employees have an obligation to be aware of, and comply with, the privacy and confidentiality laws, regulations, and TWC policies that apply to any TWC Data or TWC Information the employees use in performing their job duties.

It is important for TWC employees to keep in mind that certain privacy laws and regulations applicable to the use of TWC Data require notice to individuals regarding how their personal information will be used and, if that use changes or is different from the use described in the original consent, the affected individuals must provide an additional consent for the use of their personal information. Thus, when using TWC Data, TWC employees must be aware of the scope of the consents applicable to the TWC Data and not exceed the scope of such consent.

Furthermore, while advanced data tools can provide great benefits to TWC, TWC employees should use caution in deploying these tools to ensure that TWC Data is secure. Thus, TWC employees must configure analytics tools to protect TWC Data from unauthorized access or use and to prevent the download of TWC Data, especially TWC Data that contains PII, SPI, or PHI, either intentionally or by accident.

In accordance with these obligations, TWC employees must report to TWC management and/or (as appropriate) to TWC's Privacy Officer or FDCM:

(A) any use of TWC Data that exceeds the scope of the data subjects' consent, or

(B) any unauthorized access to or use of TWC Data.

TWC employees may also report a privacy or security event here.

2.2. Data Minimization

As noted above, TWC has a responsibility to protect the PII it collects and processes about individuals, and both legal and ethical restrictions exist on the PII TWC may share with third parties. The most effective method for protecting PII is through data minimization.

Accordingly, TWC employees:

(A) 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; and

(B) Must strive to practice data minimization and ensure they abide by any purpose limitations granted when the PII was first collected, or as expressly allowed by law.

2.3. Incomplete or Inaccurate Data; Misinterpreting Data

There are occasions where TWC employees may collect, use, or share TWC Data legally but still violate ethical standards. If TWC Data is incomplete, inaccurate, or misinterpreted, analyses and decisions based on such data may be erroneous, leading to negative impacts on individuals, communities, and the public. TWC employees must therefore exercise due diligence to identify and mitigate any potential gaps or inaccuracies in TWC Data and take proactive steps to prevent misinterpretation.

TWC employees must be keenly aware that advanced data tools and AI employ complex algorithms to analyze vast amounts of data. This can, in turn, amplify the risk that incomplete, poor-quality, or inaccurate data will lead to misleading or erroneous outputs and subsequent misinterpretation.

Therefore, in using TWC Data, TWC employees:

(A) Shall not Knowingly use incomplete or inaccurate TWC Data or Knowingly misinterpret TWC Data in the discharge of their TWC duties;

(B) Shall exercise due diligence to identify and address any incompleteness, inaccuracies, or poor quality in TWC Data before its use. If TWC Data is identified as incomplete, inaccurate, or of poor quality, employees shall either refrain from using it, or use it only with clear disclosure of its limitations and with appropriate caveats;

(C) Shall ensure that the collection, analysis, presentation, and interpretation of TWC Data, including outputs from advanced data tools and AI, minimize the risk of misunderstanding or misinterpretation. This includes designing visualizations, reports, and summaries to be clear, accurate, and free from misleading representations; and

(D) Shall document the sources, limitations, and assumptions of TWC Data and any significant analytical processes, especially when using advanced data tools or AI, to promote proper understanding of findings.

2.4. Honesty and Integrity with TWC Data

TWC employees must exhibit honesty and integrity in their work with TWC Data—regardless of job title, role, or data responsibilities—and shall not Knowingly misuse or misrepresent such data.

When sharing TWC Data and findings, TWC employees shall:

(A) Report information accurately and present any limitations or known statistical imbalances in the TWC Data;

(B) Fully disclose all sources and methods used to obtain and analyze TWC Data, including any pre-processing; and

(C) Provide detailed explanations for any exclusions and present reasonable alternative conclusions or findings, if any, based on the TWC Data.

2.5. Accountability

Ethical accountability means that TWC employees using TWC Data at any point in the data lifecycle must be aware of, and responsible to, TWC's stakeholders. Stakeholders may include TWC Data providers, such as research subjects or TWC customers, or TWC Data consumers, such as internal or external customers requesting TWC Data and information.

To comply with these ethical obligations, TWC employees shall:

(A) Handle TWC Data lawfully in accordance with Section 2.1 of this policy;

(B) Ensure compliance with TWC's agreements made with data providers and consumers regarding the use of TWC Data;

(C) Inform individuals and organizations of the potential uses of their TWC Data; and

(D) Where lawful and appropriate, allow for public access, amendment, and contestability to TWC Data and findings.

2.6. Transparency

As a state agency, TWC is subject to certain transparency standards, and thus, TWC's decision-making processes should be as transparent as possible to stakeholders. Because TWC may rely on TWC Data to make decisions, transparency depends on clear communication of all aspects of data activities throughout the entire data lifecycle. Thus, to promote transparency, TWC employees:

(A) Are encouraged to engage stakeholders through easily accessible feedback channels;

(B) Are encouraged to provide timely updates on the progress and outcomes of the use of TWC Data; and

(C) If any inaccuracies in TWC Data are discovered, TWC employees shall:
(i) document any corrections to previously reported TWC Data, and
(ii) provide explanations regarding the inaccuracies and how they were corrected.

3. Ethical Procurement, Development, Deployment, and Use of AI

AI Systems have the potential to transform the way our state and local governments serve Texans. AI Systems can create efficiencies, support economic and scientific advancement, and improve the safety and well-being of our communities. The State of Texas and TWC support the use of AI Systems by TWC employees to improve the services they deliver to Texans and to lead in innovative AI adoption in the public sector.

While they have significant potential value, AI Systems also pose substantial risks if not implemented ethically and responsibly. AI risks vary based on the system involved, how it is used, and who uses it. AI Systems are often trained on large amounts of data from a variety of sources, which can lead to inaccurate outputs. To the extent that AI Systems are trained on or used to process PII, they raise significant privacy concerns. Malicious actors can use AI to develop more advanced cyberattacks, bypass security measures, and exploit vulnerabilities in systems. These and other AI risks make it a uniquely challenging technology for TWC to use safely, but with appropriate guardrails, TWC can limit the risks of AI and secure its many benefits for TWC customers.

Applicable laws and rules require TWC to limit the potential harm of AI Systems by managing risk and prioritizing trustworthy and responsible development and deployment of AI consistent with the National Institute of Standards and Technology AI Risk Management Framework. Creating trustworthy AI requires balancing each of these principles based on the identified risks of an AI System and the context in which it is used.

This policy articulates the principles of ethical AI implementation that TWC employees must strive for when procuring, developing, designing, or using AI Systems. Additionally, TWC employees may use AI tools in the performance of their TWC job duties only in accordance with applicable laws, rules, and regulations, this policy, and the other policies mentioned in Section 1.3 above.

3.1. Ethical Development and Deployment of AI

3.1.1. Human Oversight and Control

Human oversight plays a crucial role in ensuring that AI Systems operate ethically. While AI can analyze vast amounts of data much faster—and sometimes more accurately—than humans, it lacks the human judgment necessary to ensure that its decisions align with societal values and the rights granted to individuals under the law. Ensuring human control over AI Systems mitigates risks of inaccurate or undesirable outputs and allows for revision of the rules established during development of the system and to the data that supports the system's decision-making.

Accordingly, in developing or deploying AI Systems, TWC employees:

(A) Must deploy AI Systems in ways that enable humans to review and analyze inputs and outputs at appropriate intervals throughout the AI lifecycle;

(B) Must 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

(C) Must ensure AI Systems can be disabled until harmful or inaccurate decision making can be remedied.

3.1.2. Monitoring AI Systems for Accuracy

While AI Systems are overall improving in their ability to deliver more accurate results, inaccurate outputs remain a significant risk when using AI Systems.

Accordingly, TWC employees involved in the procurement, development, or deployment of AI Systems must:

(A) Formalize processes for monitoring system accuracy before the deployment of an AI System and throughout its life cycle, as a system's accuracy may change over time; and

(B) When feasible, implement processes to improve the accuracy of AI Systems by training the systems using human feedback or improving retrieval-augmented generation by ensuring the accuracy and relevance of the underlying data used by the tool to develop answers.

3.1.3. Evaluation

AI Systems can change over time, as can the purposes for which they are used. Accordingly, in deploying AI Systems, TWC employees must:

(A) Establish methods for the regular evaluation of each AI System to ensure the system provides ongoing benefit to the populations TWC serves; and

(B) Document such evaluations.

3.1.4. Documentation

Documentation provides a critical element for managing AI risk. Consistent documentation of preliminary assessments, ongoing monitoring and testing, and complaints provides TWC with insight into the operations and improvements of its AI Systems over their life cycle. Documentation allows TWC to evaluate the value of its AI Systems and determine where best to spend resources in further developing AI solutions.

Accordingly, in deploying AI Systems, TWC employees should maintain records of:

(A) The sources of data used in the AI System; and

(B) How the AI System is modified throughout the system's life cycle.

3.1.5. Security

AI Systems are subject to security vulnerabilities. Common security concerns in the AI context involve data poisoning or malicious code injection, exfiltration of models or data within the AI System, and improper access controls that result in unauthorized access to the AI System itself. Secure AI Systems will maintain the confidentiality and integrity of the AI System as well as the data it contains even when unexpected events or changes in their environment or use occur.

Accordingly, TWC employees must:

(A) Monitor, secure, and test AI Systems to prevent or limit security attacks; and

(B) Demand that AI System providers disclose known vulnerabilities and resolutions in a timely manner to TWC.

3.1.6. Accountability and Liability in the Procurement and Deployment of AI Systems

While TWC may delegate tasks and decision making to AI Systems, TWC remains accountable for the decisions its AI Systems make and the outcomes they produce. Additionally, TWC’s use of AI Systems for employment-related tasks or to make Consequential Decisions poses heightened risks.

Accordingly, in the deployment of AI Systems, TWC employees must:

(A) Ensure the deployment of AI Systems complies with the legal obligations TWC has at both the state and federal level; and

(B) Establish appropriate records retention schedules applicable to AI Systems' records and consider the PIA's implications related to the storage of data inputs and outputs.

3.2. Ethical Use of AI

TWC is committed to leveraging AI technologies to empower employees to work more effectively and efficiently, thereby improving service delivery for TWC's customers. While TWC actively encourages employees' responsible use of AI, to harness this potential safely and ethically, employees must be aware of AI's inherent limitations. These limitations include AI's potential lack of contextual understanding, common sense, or impartiality. Additionally, TWC employees should be aware of any restrictions on the data and information that may be used even with TWC-approved AI tools. Consequently, TWC employees may use AI tools in the performance of their TWC job duties only in accordance with applicable laws and regulations, this policy, and the other policies mentioned in Section 1.3 above.

3.2.1. Restrictions on the Use of AI Systems

3.2.1.1. Never Use or Put TWC Data or TWC Information into Public AI

Public AI tools are those tools that have not been approved for use by TWC and, thus, are accessible only because the tool has been made available to the general public. Examples of such tools include Grok, Perplexity, and the public version of Google Gemini. Importantly, because unapproved AI tools are not secure, and such tools may use inputs to train the model and share those inputs with other users of the public AI tool, TWC employees **must not use public AI tools** in connection with their TWC job duties. Most importantly, as required by Section 3.2.7, TWC employees **must never put PII into a publicly available AI tool**.

3.2.1.2. Use Only TWC-Approved AI

In performing their work duties, TWC employees are authorized to use only TWC-approved AI Systems because those tools have been vetted and deployed in a way to protect the integrity and confidentiality of inputs and outputs and to protect TWC Data and TWC Information from unauthorized or unlawful disclosure or use (see Section 2.1 and Section 3.2.7). TWC

employees should consult the list of TWC-approved PC software (TAPS list) to determine whether an AI tool is approved for use by TWC employees. (Employees may also consult the list of TWC-approved AI tools, but such list is not definitive; the TAPS list is the definitive source for approved AI tools, as well as any restrictions on the data and information that may be used with such tools (see Section 3.2.1.4 below).)

TWC employees with AI-related questions may contact the Software Acquisition Review Committee (SARC) Coordinator (sarc@twc.texas.gov) or the AI Team (ai@twc.texas.gov), who are always available to assist. Employees may also find general information on AI on the Information Technology Division's Artificial Intelligence SharePoint page.

3.2.1.3. Unapproved AI Tools in Approved Software

Software vendors frequently introduce new AI capabilities into previously approved TWC software applications. The prior approval of a software product **does not**, however, automatically extend to newly added AI features.

TWC employees **must not** enable, test, or use newly introduced AI tools within existing software until they receive explicit approval from the Information Technology Division.

To request a review or verify the approval status of a new AI tool, TWC employees must contact the SARC coordinator by:

- Emailing sarc@twc.texas.gov or
- Submitting an IT software portal ticket.

Additionally, because vendors may automatically activate new AI features without notification or warning, employees who discover an unannounced AI capability within existing software must refrain from using it and immediately report its presence to the SARC coordinator. If an employee inadvertently uses a new AI feature that was enabled by a vendor without notification or warning, the employee shall not be deemed to have taken wrongful action, provided they immediately cease use of the tool upon discovery of the unapproved AI capability and promptly report the feature to the SARC coordinator.

3.2.1.4. Data Restrictions with TWC-Approved AI

Even if an AI tool has been approved for use by TWC employees, there may be restrictions on the data or information that employees may use with such

tools. The TAPS list includes the data and information restrictions applicable to TWC-approved AI tools.

For example, there is an **absolute prohibition on** the use of certain **federally restricted data** with even TWC-secured AI tools.
This includes the following types of data:

- **CJIS** (Criminal Justice Information Security) data,
- **FERPA** (Family Educational Rights and Privacy Act) data,
- **FTI** (Federal Tax Information) data, or
- **SSA** (Social Security Administration) data.

Note: The above restriction does not apply to data that comes directly from the customer. It does, however, apply to data that comes from the original federal or educational source or an authorized secondary source and includes data TWC derives from those sources. Importantly, even if the data does not qualify as federally restricted data, it is still PII, and data minimization principles apply.

As noted in Section 2.2, TWC employees must practice **data minimization** with respect to PII. Because AI inputs and outputs are retained for 14 days, this means that using PII with approved AI tools will result in additional copies of any PII used with an approved AI tool. Thus, TWC employees should **minimize the use of PII with TWC-approved AI tools** and use of PII with AI only to the extent absolutely necessary as part of their TWC job duties.

3.2.2. Human Review of AI Output Required

While AI Systems are overall improving in their ability to deliver more accurate results, inaccurate or misleading outputs remain a significant risk when using AI Systems. TWC employees must be aware of this potential and must review all AI output used in any TWC work product.

3.2.2.1. Review of AI Output for Accuracy

TWC employees must review any AI content used in their work product with a heightened level of scrutiny to ensure any TWC work product is accurate. If a TWC employee is **unable to verify the accuracy** of the AI content through an independent credible source, which may include formal or

informal consultations with peers or supervisors, the TWC employee **must not use** that content in any TWC work product.

Additionally, to improve TWC's processes, if an employee notices an error, the employee should report it to the appropriate administrators. For TWC-developed AI tools, contact TWC's IT AI team at ai@twc.texas.gov.

3.2.2.2. Human Review Required for Consequential Decisions

Texas law requires TWC to follow additional strict rules if AI makes Consequential Decisions autonomously. You must therefore understand that you **cannot let an AI tool make consequential decisions by itself**.

A **"consequential decision"** is one that has a material legal or similarly significant effect on the provision, denial, or conditions of a person's access to a government service. **Simply put, this is a decision that can change whether someone receives or is denied a TWC benefit or service or the conditions someone must meet before receiving a benefit or service.** Examples of a Consequential Decision by TWC would include (but are not limited to) using an AI System—by itself—to determine:

- Eligibility for grant funds, unemployment compensation benefits or vocational rehabilitation services;
- Whether an employment or housing discrimination complaint is actionable; or
- Licensing decisions for career schools.

Thus, if TWC employees use approved AI tools to **help analyze** Consequential Decisions, employees must **always check the AI's answers very carefully** to determine, using their own independent judgment:

- Is the AI output correct?
- Is the AI output's conclusion based on complete information, including all necessary facts and conditions?
- Does the AI output align with TWC policies and applicable law?

Remember: Each **TWC employee is responsible** for his or her own work product, including any Consequential Decisions. Each Consequential Decision an employee makes must result from **the employee's own independent professional judgment**—it cannot be a simple copy/paste of AI output without meaningful human review.

TWC employees seeking to use an AI tool to autonomously make a Consequential Decision must first contact the AI Risk Office because any such use must meet specific statutory and regulatory requirements. The AI Risk Office can provide additional guidance on this process.

3.2.3. Employees Are Responsible for AI Use in TWC Work Product

If TWC employees use AI-generated content in their work product, they must be prepared to provide an honest answer about its use and an honest explanation of all decisions made in connection with that use, including whether they employed critical thinking to determine whether the AI output is accurate and aligns with applicable law and TWC policies. It is recommended that staff proactively disclose the use of AI in generating content for work products in the following scenarios:

- The AI tool generates substantive portions of the text;
- The work product directly incorporates or replicates AI-generated content; or
- The AI tool substantively shapes the core arguments or findings in the work product.

Ultimately, each TWC employee is responsible for his or her own work product. If that work product contains AI-generated content, it is assumed that the employee has reviewed that content for accuracy and alignment with applicable laws and TWC policies. Failure to do so does not relieve an employee from the consequences of inaccurate, damaging, or incomplete TWC work product.

Failure to follow this Section 3.2.3 would not only violate this policy but could also violate potentially applicable laws and regulations or various sections of the TWC Ethics Policy (e.g., Section 1.10.2.11 regarding providing false information in the course of official business).

3.2.4. Fairness

Any TWC Data used to develop AI Systems must adequately represent the subjects or people about which such systems make judgments, decisions, or predictions. Incomplete or inaccurate TWC Data can result in Unlawful Harm.

Accordingly, TWC employees must:

(A) Ensure their use of AI Systems does not infringe upon the legally protected rights and liberties of the individuals they serve or result in Unlawful Harm; and

(B) Implement data governance practices for AI Systems throughout the AI System's life cycle to ensure fairness.

3.2.5. Redress

Providing a method for redress will promote public trust in both the relevant AI System and in TWC. Therefore, if a TWC employee identifies any negative impacts caused by the use of AI Systems, the employee must report that impact to the AI Risk Office (ai.riskoffice@twc.texas.gov). Employees must also report any violation of this policy or the laws and rules applicable to AI Systems by TWC employees, contractors, or vendors to the AI Risk Office. Technical issues involving AI should be reported to the IT AI team (ai@twc.texas.gov).

Additionally, if TWC deploys a Heightened Scrutiny AI System, TWC employees must ensure that they:

(A) Provide a mechanism to seek redress for those impacted when an AI System makes a Consequential Decision that unfairly impacts an individual or group in a material way; and

(B) Designate a point of contact for individuals to address when seeking information about an unfair Consequential Decision.

3.2.6. Transparency

Establishing transparency for AI Systems means providing information about the data, models, and outputs of an AI System to both the individuals interacting with the AI System and those deploying it. Strong transparency practices will build public trust in TWC’s AI Systems.

Accordingly, TWC employees must:

(A) Collaborate with developers of AI Systems and demand transparency to understand how an AI System operates, the source of the data the AI System was trained on, and its intended use cases;

(B) Strive to understand the capabilities of the AI System and how it makes decisions;

(C) Disclose when individuals interact with an AI System and when an AI System is used to make Consequential Decisions about such individuals' rights or access to TWC services; and

(D) Never represent AI Systems as human when interacting with the public.

3.2.7. Data Privacy

Information entered into AI Systems may be used to train the tool or shared with other users as output. Additionally, many AI Systems rely on vast amounts of PII to make predictions and decisions. Thus, it is important to keep in mind the data privacy principles discussed in Section 2.1 because those principles also apply to the PII TWC processes in and shares with AI Systems. TWC employees should be aware that sharing PII with an AI tool may violate privacy laws and obligations TWC has to the applicable individuals, particularly if an AI tool is used outside TWC's secure environment.

Accordingly, TWC employees must strive to understand what PII AI Systems use, how that PII has been and will be collected, and how the tool uses, stores, and shares PII with third parties prior to using any government-held PII in an AI System. In light of these obligations, TWC employees must:

(A) Never use TWC Data or TWC Information (including any SPI and PII contained therein) with public AI tools;

(B) Ensure that any use of AI is secure and configured to protect TWC Data and TWC Information from unauthorized access or use; and

(C) Ensure AI tools do not train models, share, or sell TWC Information or TWC Data outside of TWC's control.

3.2.8. Accountability and Liability

While TWC may delegate tasks and decision making to AI Systems, TWC remains accountable for the decisions its AI Systems make and the outcomes they produce. TWC's use of AI Systems for employment-related tasks or to make Consequential Decisions poses heightened risks.

Accordingly, TWC employees must:

(A) Understand how to use AI Systems in an effective, safe, and ethical way;

(B) Ensure the deployment of AI Systems complies with the legal obligations TWC has at both the state and federal level; and

(C) Abide by TWC's records retention schedule applicable to AI Systems' records and be mindful of the PIA's implications related to the storage of data inputs and outputs.

3.2.9. Any Heightened Scrutiny AI System Must Follow AI Minimum Standards

If TWC determines to deploy a Heightened Scrutiny AI System, TWC employees shall ensure the system meets all the requirements set forth in 1 Texas Administrative Code §§ 219.21-219.24.

TWC employees seeking to deploy a Heightened Scrutiny AI System must first contact the AI Risk Office because any such use must meet specific statutory and regulatory requirements. The AI Risk Office (ai.riskoffice@twc.texas.gov) can provide additional guidance on this process.