Fort Bend County Artificial Intelligence Policy

Introduction

This policy defines the proper use of Artificial Intelligence (AI) within Fort Bend County and establishes standards for its responsible, transparent, and ethical use. It is subject to revision as AI guidelines, laws, and technologies evolve.

Fort Bend County is committed to aligning its AI practices with recognized local, global, and national frameworks for trustworthy and responsible AI, including but not limited to:

- The NIST AI Risk Management Framework (AI RMF 1.0, Jan. 26, 2023),
- ISO/IEC 23894:2023 (Guidance on AI Risk Management), and
- Blueprint for an U.S. AI Bill of Rights
- HB 149 (the Texas Responsible Artificial Intelligence Governance Act - TRAIGA), effective January 1, 2026
- And other relevant federal or state directives.

These frameworks will guide the County's AI governance, risk management, and training programs to ensure consistency, transparency, and continuous improvement.

This policy applies to all Fort Bend County employees, elected officials, contracted individuals, interns, and vendors who use artificial intelligence (AI) tools or systems in the course of their official duties.

Fort Bend County is committed to developing, deploying, and managing AI technologies in a human-centric, trustworthy, secure, and compliant manner that upholds County values, protects public trust, and ensures equitable service delivery. All AI use must align with applicable laws, regulatory standards, and recognized best practices for responsible AI governance.

The term "Artificial Intelligence" or "AI" has the meaning outlined in 15 U.S.C. § 9401(3): a machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations, or decisions that influence real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments, abstract these perceptions into models through automated analysis, and use model inference to formulate options for information or action.

Fort Bend County's Relationship with Machines

Ownership

Fort Bend County employees, elected officials, contracted individuals, interns, and vendors using AI are individually responsible for ensuring the accuracy, integrity, and ethical use of AI in their work. They must be able to clearly and accurately explain AI-assisted outputs and promptly notify the County if unable to do so.

Individual ownership includes maintaining awareness of how AI systems are used, validating AI-generated outputs, and ensuring that all work products remain aligned with County values, applicable laws, and ethical standards.

To complement this individual accountability and to ensure organization-wide consistency, oversight, and continuous improvement, Fort Bend County has established the Emerging Technologies Committee as part of its broader AI governance framework.

Emerging Technologies Committee

The Emerging Technologies Committee (ETC) provides centralized oversight, coordination, and accountability for the responsible use of Artificial Intelligence (AI) across all County departments, offices, and vendor partnerships.

Purpose and Responsibilities

The Committee's key responsibilities include:

- Oversight and Policy Enforcement: Monitor County-wide AI compliance and ensure all uses align with ethical, legal, and regulatory standards.
- Risk and Incident Review: Evaluate AI-related incidents, potential misuse, or breaches; determine root causes; and recommend corrective or preventive measures.
- Approval and Exception Authority: Review and approve proposed AI use cases, vendor tools, and requests for variances from policy or restrictions.
- Training and Awareness: Support County-wide training and awareness initiatives to promote responsible and ethical AI use.
- Continuous Improvement: Recommend updates to AI policies, processes, and safeguards based on technology changes, audit results, or best practices.

Membership and Structure

The Emerging Technologies Committee includes key representatives from Fort Bend County Information Technology to provide oversight, technical expertise, and accountability in AI governance and implementation.

Core Members (IT Department):

- IT Security Manager: Ensures compliance with cybersecurity, privacy, and data protection standards.
- Applications Team: Supervisor, Manager, and two Senior Programmer Analysts overseeing AI configuration and integration.
- PMO Representative: Manages project coordination, timelines, and risk tracking.
- Network Engineer (voice): Reviews infrastructure readiness and system performance for AI systems.
- Systems Programming Team: One Systems Programmer supporting technical implementation and integration.

Additional Members (As Needed):

Representatives from Legal, Human Resources, Procurement and Finance, Office of Emergency Management (OEM), and Public Information/Communications may participate depending on project scope, risk, or operational relevance.

Decision Rights and Escalation

- The Committee has the authority to approve, restrict, or suspend AI tools, systems, or practices that do not comply with County policy or security standards.
- Moderate- to high-risk AI approvals must also be reviewed by the Change Control Board (CCB) to ensure alignment with enterprise change management and system integrity requirements.
- All major decisions, approvals, and recommendations will be documented for accountability and audit purposes.
- The Committee will meet quarterly, or more frequently as needed, to review AI activities, assess incidents, and evaluate the overall risk posture of AI use across the County.
- Significant risks or exceptions may be escalated to the Commissioners Court for final ratification or policy variance approval.

AI Approval and Exception Process

Departments seeking to use new or restricted AI capabilities must submit a request to the Emerging Technologies Committee (ETC) before deployment. Each request must include:

- The AI system name and purpose
- Intended use and data to be processed
- Risk assessment and justification for use

Review Process

- Low-Risk Requests (e.g., internal productivity tools) may be approved directly by the ETC.
- Moderate- to High-Risk Requests (e.g., systems handling sensitive data or public-facing AI) require ETC approval and subsequent Change Control Board (CCB) review before implementation.
- The ETC may apply additional safeguards or monitoring requirements to any approved AI tools or use cases.
- The Commissioners Court must ratify policy exceptions or variances following the Committee's recommendation.

Recordkeeping and Review

- All requests, decisions, and approvals must be documented and retained by the IT Department for audit purposes.
- Approved AI tools and exceptions must include a defined review date and are subject to periodic reauthorization by the ETC.

Accuracy and Accountability

Employees, elected officials, contracted individuals, interns, and vendors utilizing AI must ensure content accuracy and maintain accountability in official communications and interactions. While Generative AI may enhance productivity and efficiency, employees, elected officials, contracted individuals, interns, and vendors must exercise their professional judgment and expertise to validate any AI-generated work output.

Transparency and Explainability

Fort Bend County employees, elected officials, contracted individuals, interns, and vendors using AI must disclose any use of AI-generated content in reports, communications, and external interactions.

AI Usage Documentation
Users must maintain documentation outlining their AI workflow and points of human oversight. This should describe:

- The types of data or inputs used,
- The purpose and nature of AI outputs, and
- Where human review or approval occurs ("human-in-the-loop" or "human-on-the-loop").

Departments must be able to provide this documentation upon request to demonstrate responsible, supervised AI use. All records must comply with County records management and data governance policies.

For AI systems that extend beyond generative content (for example, decision-support, predictive, or classification models), additional documentation must include:

- **Model Logic and Design:** A summary of how the model functions, including algorithms, data inputs, and decision pathways.
- **Decision Rationale:** An explanation of how and why the AI system produces specific outputs, recommendations, or actions.
- **Known Limitations and Risks:** Identified constraints, performance thresholds, or conditions under which the AI may be unreliable, biased, or incomplete.
- **Validation and Testing Evidence:** Records demonstrating that AI systems have been reviewed, tested, and verified for accuracy, fairness, and consistency with County standards.

All documentation must be made available to the Emerging Technologies Committee or designated oversight authority upon request. The Committee will periodically review these records to verify transparency, explainability, and compliance with County and regulatory requirements.

Prohibition of Sole Reliance

Fort Bend County employees, elected officials, contracted individuals, interns, and vendors must not rely solely on AI for conclusive decisions.

If AI is being used as a decision-support tool, all outputs must be reviewed and validated by a qualified human to ensure accuracy, ethical compliance, and alignment with County policies.

If AI is being used for decision-making or automation capabilities (e.g., advanced or agent-based AI systems), a **human-in-the-loop or human-on-the-loop mechanism** must be established to maintain oversight and accountability. These mechanisms must allow authorized personnel to

review, approve, or override AI-generated actions or recommendations before they are finalized or implemented.

All AI-assisted decisions must be documented, and any errors, anomalies, or risks identified in AI outputs must be promptly reported for investigation and resolution. Human judgment, transparency, and accountability remain central to all decision-making processes involving AI, particularly in high-impact areas such as employment actions, financial determinations, and public service delivery.

Prohibition of Harmful Activities

Generative AI is strictly prohibited from use in activities that are harmful, unlawful, unethical, discriminatory, or in violation of County policies. All AI technologies must adhere to legal and ethical standards to protect the County, its personnel, and the public.

AI Restrictions

The Fort Bend County Information Technology (IT) Department maintains a list of approved and restricted AI activities and technologies. Employees, elected officials, contracted individuals, interns, and vendors must always comply with this list. To obtain the most current version, contact the Fort Bend County IT Department.

Responsibilities

All County personnel, elected officials, contracted individuals, interns, and vendors using AI, including Generative AI, are responsible for reviewing this policy to understand the risks of using AI and Generative AI and how to use them in accordance with this policy.

The Public's Relationship with Machines

Public AI Used Within Fort Bend County Website and Applications

Fort Bend County may use third-party AI to improve customer service. The County will prominently disclose the use of any third-party AI and provide clear information on its purpose and scope of use. The AI services are offered exclusively for customer service assistance and are not designed to perform decision-making tasks or provide legal advice.

Public Complaint and Dispute Resolution:
Fort Bend County will establish a formal process to address complaints or disputes related to AI interactions, enhancing transparency and trust. This includes:

1. Complaint Submission: A contact point (such as the Fort Bend County IT Service Desk at 281-341-4580 or it.servicedesk@fbctx.gov) where users can submit concerns about AI interactions, including inaccuracies, misrepresentations, or inappropriate outputs.

2. Complaint Review: A designated team will review complaints and determine their validity and severity.

3. Response Timeline: Fort Bend County will reasonably respond to complaints and, as applicable, clarify actions to address the concern.

4. Corrective Measures: If an AI is found to have caused harm or issued incorrect outputs, Fort Bend County will work with the third-party AI provider to correct the issue and improve system performance.

AI Incidents

AI-Related Incidents and Handling Procedures

An AI-related incident is any event or action involving the use of Artificial Intelligence (AI) that results in negative consequences for Fort Bend County, whether operational, financial, reputational, or legal.
This procedure aligns with the Fort Bend County Incident Response Plan (Rev 1.4) and follows the same NIST SP 800-61 r2 life-cycle stages: *Preparation, Detection & Analysis, Containment, Eradication & Recovery, and Post-Incident Review*.

Examples of AI-Related Incidents

1. Data Breach or Unauthorized Access: Exposure, loss, or misuse of County or citizen data caused by an AI system or model.
2. Misrepresentation of Information: Biased, inaccurate, or misleading AI outputs that result in reputational or operational harm.
3. Operational Failures: System malfunction or unauthorized AI use disrupting County services or automation.
4. Legal or Compliance Violation: Use of AI resulting in non-compliance with privacy, accessibility, or regulatory requirements.
5. Harmful Decision-Making: AI recommendations causing adverse human, safety, or employment impacts.
6. Financial Impact: Measurable fiscal loss due to AI errors, misuse, or vendor non-performance.

1. Detection and Reporting

- Immediate Notification
  Upon discovery of an AI-related incident, the responsible individual (employee, official, contractor, intern, or vendor) must immediately contact the Fort Bend County IT Service Desk at 281-341-4580 or it.servicedesk@fbctx.gov.
- Ticket Creation:
  The IT Service Desk will open a ServiceNow incident ticket using the *Cybersecurity Incident*

form type. “AI-Related Incident” will be entered in the memo field and cross-referenced to the affected system or department.

- Escalation to CIRT:
  The Cyber Incident Response Coordinator (CIRC) and IT Security Manager will determine severity and coordinate activation of the Cyber Incident Response Team (CIRT) in accordance with the County’s priority matrix.

2. Classification and Severity Levels

Priority Level	Impact Description	Response & Escalation
Level 0 – Low	Minor AI misclassification or data error with no sensitive data involved.	Logged and resolved by the business unit and the IT Service Desk. Reviewed during the next Committee meeting.
Level 1 – Moderate	AI output or automation causes operational inefficiency or reputational risk, and limited data exposure.	Escalate to the Emerging Technologies Committee and the CIRC for review and remediation.
Level 2 – High	AI misuse or error affecting multiple departments, sensitive data, or regulatory compliance.	Immediate activation of CIRT; Legal Counsel, HR, and Communications engaged; follow IRP containment and notification protocols.
Level 3 – Critical	Major service disruption, public-facing harm, or safety impact; confirmed breach of sensitive information.	Full IRP activation. County Administrator, CIO, and Commissioners Court notified. Incident declared enterprise wide.

Severity classification must consider confidentiality, integrity, and availability impacts consistent with the CIA Triad (see Section “Impact Definitions and Potential Risk,” IRP Rev 1.4).

3. Containment, Eradication, and Recovery

Containment and recovery activities for AI incidents follow the same methodology as the County’s IRP:

1. Containment: Temporarily disable affected AI modules or automation scripts; isolate impacted systems to prevent propagation.
2. Eradication: Remove corrupted or compromised AI components, retrain models if necessary, and revoke unauthorized access credentials.
3. Recovery: Restore validated models and services from clean backups or verified repositories; monitor for recurrence.

All actions, timestamps, and responsible personnel must be recorded in the incident ticket and retained in accordance with IRP documentation requirements.

4. Communication and Coordination

- The CIRT, in coordination with Community Relations and Legal Counsel, will manage internal and external communications.
- If an AI incident involves citizen data or public impact, breach notification procedures outlined in the IRP (§ Breach Notification, p. 14) must be followed.
- The Emerging Technologies Committee will provide subject-matter oversight for AI-specific risk factors and report findings to the CIO and County Administrator.

5. Post-Incident Activity and Continuous Improvement

After containment and recovery, the CIRT and Emerging Technologies Committee will jointly conduct a Post-Incident Review (PIR) to:

- Assess the root cause, system weaknesses, and human factors involved.
- Recommend updates to AI governance policies, training, or technical safeguards.
- Determine if further legal or regulatory reporting is required.

Findings and remediation plans must be documented using the IRP's *Post Incident Activity and Review Form* and maintained by IT Security.

6. Linkage to Existing County Plans

This section operates as an addendum to the Fort Bend County Incident Response Plan (Rev 1.4) and leverages the same:

- Incident lifecycle (Preparation → Detection → Containment → Recovery → Post-Incident Review)
- Roles and responsibilities (CIRC, CIRT, IT Security Manager, Legal Counsel, Communications Officer, HR Director, OEM Coordinator, etc.)
- Reporting and documentation templates (Detection, Analysis, Containment, Eradication, Recovery, Post-Incident Activity Forms).

AI incidents will be tracked within the same incident-management system as cybersecurity incidents, ensuring consistency, accountability, and audit readiness.

Data Regulations

Intellectual Property

Fort Bend County owns all data it gives to AI and receives from AI.

Fort Bend County prohibits any unauthorized utilization of copyrighted materials, trademarked materials, and/or any proprietary data.

If a vendor does not agree to transfer ownership of any AI data outputs to the County, the vendor must secure and obtain a policy variance from Information Technology.

Confidential Data

PHI (Protected Health Information) or PII (Personally Identifiable Information) shall not be provided when interacting with AI.

Unless suitable enterprise controls and data protections are in place as determined by the County's IT Department, County elected officials, employees, contractors, interns, and/or vendors should not insert Confidential Data into third-party, cloud-based Generative AI models or applications. Information entered into Generative AI models or applications can be made available to the public and later users, potentially rendering the County unable to shield it from disclosure.

Data Containment and Harm Mitigation:

To govern the use of public-facing AI and mitigate risks, Fort Bend County will implement data containment mechanisms and continuous model testing to ensure responsible AI behavior, including:

- Guardrails to Prevent Harm: Regular reviews of AI-generated outputs to ensure compliance with County guidelines and avoid potential harm to users.
- Continuous Model Testing: Ongoing testing of AI models to detect and mitigate issues such as hallucinations (generating false or misleading information).

- Incident Response Protocols: Predefined procedures to address and resolve issues arising from AI interactions, including immediate containment of erroneous outputs and corrective updates to the AI system.

Data Protection

Employees, elected officials, contracted individuals, and interns must maintain the confidentiality and security of all County information, including, but not limited to, adhering to all applicable policies, administrative regulations, contractual obligations, and legal obligations.

Public Information Act

All information and any product created by Generative AI models or applications, including information inserted into County documents, should be considered to be public information and may be subject to a Public Information Act request. However, before any required disclosure, any sensitive, confidential, or protected information must be appropriately reviewed and redacted in accordance with County policies and applicable laws.

Enforcement Procedures

To ensure adherence to the data minimization principle, the following procedures will be implemented:

1. Needs Assessment

- Before integrating or deploying AI systems, County offices and departments must conduct a Data Needs Assessment to identify the minimum data required for the intended purpose.
- Only data explicitly necessary for achieving the defined objectives of the AI system will be approved for use.
- Data must be stored in accordance with applicable laws and County record retention parameters, but not retained longer than necessary.

2. Approval Process

- All AI-related data collection processes must be reviewed and approved by Fort Bend County's Emerging Technologies Committee or an equivalent oversight authority.
- Justification for each data element collected must be documented and submitted as part of the review process.

3. System Configuration

- Technical safeguards that limit or anonymize data inputs, such as field masking, pseudonymization, or aggregation, should be implemented to reduce identifiable information.
- AI systems should include configurable retention controls to automatically purge or anonymize data upon meeting retention limits.

4. Monitoring

- Continuous Monitoring: Departments must establish Key Performance Indicators (KPIs) or metrics to track ongoing adherence to data minimization principles, including:
    - Volume of data collected versus data authorized for use,
    - Retention duration trends and exceptions,
    - Frequency of data access by AI models or users,
    - Compliance rate with data deletion or anonymization schedules, and
    - Incidents involving overcollection or unnecessary retention.
- Metrics should be reviewed by the Emerging Technologies Committee and IT Security team to detect emerging risks, inefficiencies, or systemic policy deviations.

5. Continuous Improvement

- AI governance procedures will be reviewed annually and updated as needed based on feedback, regulatory changes, and emerging best practices.

Security

Security and Privacy

The policy mandates rigorous data protection measures to ensure compliance with privacy regulations. All data submitted to AI systems must be handled securely to prevent unauthorized access or disclosure, and users must demonstrate strict control over system input data.

Any use of Generative AI should comply with all County policies and standards regarding information security, including, but not limited to, password protection and data encryption.

Secure Development Practices

Generative AI models and applications must be developed in accordance with Fort Bend County's Secure Software Development Life Cycle (SDLC) and related information security standards. All AI systems must follow the same secure design, development, testing, and deployment procedures applied to other County technology projects.

AI solutions must incorporate secure coding practices and undergo rigorous testing, including vulnerability scanning, static and dynamic code analysis, penetration testing, and peer code reviews, to identify and mitigate security vulnerabilities.

Developers and project teams must ensure that:

- Security and privacy controls are implemented at each SDLC phase, from design through deployment.
- Dependencies, APIs, and open-source components used in AI models are regularly reviewed for known vulnerabilities.
- Changes or updates to AI systems follow established change control and configuration management processes.
- Security documentation, test results, and approvals are maintained for audit and compliance verification.

These measures ensure that all AI technologies remain resilient against cyber threats, maintain the integrity and confidentiality of data, and uphold the County's enterprise security standards.

Third-Party Security Evaluation

Fort Bend County must conduct comprehensive security evaluations of third-party Generative AI tools or services to ensure compliance with County security standards. Evaluations include

reviewing vendor security certifications, performing security assessments, and establishing contractual agreements to address security requirements and mitigate risks.

Vendor Disclosures

Disclosing the Use of AI

Vendors must prominently disclose their use of AI in their contracts or a designated section of their documentation. The disclosure must include:

1. **Specific AI Used:** A detailed description of the AI employed, including its purpose and capabilities.

2. **Nature of Use:** Explain how the AI is utilized for Fort Bend County operations, services, or deliverables.

3. **Content Identification:** Any content directly produced by an AI must be explicitly identified as AI-generated in reports, documentation, or deliverables.

If a vendor does not agree to the terms of disclosure, then the vendor must secure and receive a policy variance from Information Technology.

Policy Violations

Vendor Accountability for Policy Violations:
To ensure adherence to this policy, vendors will be held accountable for any violations of the AI disclosure or usage requirements:

1. **Contractual Obligation:** Non-compliance with AI disclosure requirements will be considered a breach of contract, subject to penalties outlined in the vendor agreement.

2. **Financial Penalties:** Vendors may be required to compensate Fort Bend County for any damages, additional costs, or disruptions caused by non-disclosure or misuse of AI.

3. **Suspension of Engagement:** Depending on the severity of the violation, vendors may face suspension or termination of their contracts with Fort Bend County.

4. **Remediation Requirements:** Vendors found in violation must submit a detailed remediation plan within a specified timeframe, outlining corrective actions to prevent future breaches.

5. **Audits and Monitoring:** Fort Bend County reserves the right to conduct audits of vendor AI usage to ensure compliance with this policy. Vendors must fully cooperate with these audits and provide the necessary documentation.

Employee, Contractor, and Intern Accountability for Policy Violations:
To ensure adherence to this policy, employees, contracted individuals, and interns will be held accountable for any violations of the AI disclosure or usage requirements.

1. **Contractual Obligation:** Non-compliance with AI disclosure requirements by employees, contractors, and interns will be considered a breach of contract.

2. **Disciplinary Procedures:** Depending on the severity of the violation, employees, contracted individuals, and interns may face disciplinary action, up to and including termination of employment.

3. **Withdrawal of Access:** Depending on the severity of the violation, Fort Bend County may withdraw access to the applicable AI.

4. **Remediation Requirements:** Employees, contracted individuals, and interns found in violation must submit a detailed remediation plan within a specified timeframe, outlining corrective action to prevent future breaches.

5. **Audits and Monitoring:** Fort Bend County reserves the right to conduct an audit of employee, contractor, and intern AI usage to ensure compliance with this Policy. Employees must fully cooperate with these audits and provide the necessary documentation.

Elected Officials' Accountability for Policy Violations:
To ensure adherence to this policy, elected officials will be held accountable for any violations of the AI usage requirements.

1. **Withdrawal of Access:** Depending on the severity of the violation, Fort Bend County may withdraw access to the applicable AI.

2. **Remediation Requirements:** Elected officials found in violation must submit a detailed remediation plan within a specified timeframe, outlining corrective action to prevent future breaches.

3. **Audits and Monitoring:** Fort Bend County reserves the right to conduct audits of elected officials' AI usage to ensure compliance with this Policy. Elected officials must fully cooperate with these audits and provide the necessary documentation.

Authorized Access
Employees, elected officials, contractors, interns, and vendors using AI must strictly adhere to relevant laws, regulations, and policies governing their use in official County-related activities. They are also responsible for the proper use, care, and security of all AI.

If an employee, elected official, contractor, intern, or vendor does not adhere to this policy, access to AI may be withdrawn.

Evaluation of AI

AI Inventory

Fort Bend County will maintain a centralized, regularly updated inventory of all Artificial Intelligence (AI) systems, applications, and tools in use across County departments, offices, and vendor partnerships. This inventory functions as the official record of AI usage and supports oversight, risk management, compliance monitoring, and transparency.

Each entry in the AI Inventory must include the following information:

1. **AI Tools in Use:** A comprehensive list of all AI systems employed by the County, including their name, purposes, scopes, expected outcomes, and areas of application.
2. **Vendor Information:** Identification of third-party vendors providing AI systems or services, including contract details, licensing, data-sharing provisions, and security or compliance certifications (such as FedRAMP, ISO 27001, or SOC 2).
3. **Functionality and Performance:** A summary of each AI system's primary functions, performance metrics, limitations, and dependency relationships with other County systems.
4. **Data Handling:** Documentation must describe how each AI system collects, processes, stores, and transmits County data, indicate whether it trains or fine-tunes on that data, and confirm compliance with the County's Data Protection, Data Minimization, and Confidential Data provisions.
5. **Classification by Context, Risk, and Business Function:** Each AI system will be classified by its operational context (department or program), use case (such as automation, analysis, or decision-support), risk level (low, moderate, or high), and impact tier. The impact tier identifies systems that influence public services, personnel actions, finances, or critical operations and therefore require heightened review and oversight.

Inventory Oversight and Maintenance

The Emerging Technologies Committee, in coordination with the IT Department, is responsible for maintaining and verifying the accuracy of the AI Inventory. Departments must submit updates within 30 days of deploying, modifying, or retiring any AI system.

All updates will be reviewed for compliance with the AI Restrictions and Exception Process and, when applicable, the Secure Development Practices requirements. The Committee will conduct quarterly reviews to assess system performance, risk, and compliance, and to ensure each AI system maintains appropriate transparency, explainability, and human oversight.

High-risk or non-compliant systems will receive additional oversight, which may include independent validation, bias assessments, or third-party audits, consistent with the Incident Handling and Prohibition of Sole Reliance provisions of this policy.

Periodic Reviews for Alignment and Adaptability:

To ensure AI systems remain aligned with Fort Bend County's operational, ethical, and strategic goals, the AI Inventory will undergo periodic reviews coordinated by the Emerging Technologies Committee.

The scope and frequency of these reviews will be **proportionate to each system's risk and impact level**. High-risk or high-impact systems will receive more frequent and detailed evaluations, while low-risk systems will be reviewed on a scheduled cycle or as needed.

Reviews will include the following focus areas:

1. **Goal Alignment:** Confirm that each AI system continues to support County objectives, values, and public service outcomes.
2. **Technology Updates:** Assess whether current AI tools remain effective, secure, and relevant as technology evolves.
3. **Performance and Risk Monitoring:** Evaluate accuracy, efficiency, bias, and operational reliability using defined metrics.
4. **Compliance Validation:** Ensure continued adherence to County policies, applicable regulations, and security standards.
5. **Stakeholder Feedback:** Gather input from County employees, officials, and departments to identify challenges, opportunities, and evolving needs.

Actionable Outcomes:
AI tools found to be misaligned, underperforming, or non-compliant may be flagged for corrective action, update, replacement, or decommissioning. Review findings will inform continuous improvement recommendations and risk management priorities to maintain alignment with County goals.

Professional Development

Training and Awareness

Employees, contractors, and interns must participate in mandatory and role-specific training programs to gain a comprehensive understanding of AI technology, including its capabilities, limitations, biases, and potential risks. This training is critical for fostering responsible and effective use of AI within Fort Bend County.

Key Training Objectives:

1. **AI Fundamentals:** Provide an overview of how AI works, its functionalities, and its roles in County operations.
2. **Understanding Limitations:** Highlight AI's limitations, such as its reliance on data quality, potential inaccuracies, and lack of human judgment.
3. **Bias Identification and Mitigation:** Educate participants on the risks of bias in AI systems and how to recognize and address such issues.
4. **Risk Awareness:** Inform employees, contractors, and interns about the potential risks of AI use, including security vulnerabilities, misuse, and unintended consequences.
5. **Ethical Use and Compliance:** Reinforce adherence to County policies, regulations, and ethical guidelines for AI usage.

Societal Adaptation

Responding to Rapid Change

Fort Bend County will continuously monitor advancements in Artificial Intelligence and related technologies to assess their potential benefits, risks, and impacts on County operations. The Emerging Technologies Committee will periodically review emerging tools and recommend safe, ethical, and effective adoption strategies.

Regular Document Updates

Fort Bend County will regularly review and update this AI Policy to ensure it remains current and effective. Updates will be made as needed to reflect technological advancements, regulatory or legislative changes, audit findings, incident reviews, risk assessments, and organizational changes affecting AI use or oversight.

Emerging ethical considerations, vendor or contractual updates, new County initiatives, or feedback from the Emerging Technologies Committee may also trigger policy revisions. These updates ensure continued alignment with industry best practices, County values, and evolving legal and compliance requirements.

Discretionary Authority

Fort Bend County reserves the right to reject a vendor's use of AI if it does not comply with County policy. This discretionary authority ensures that AI implementations align with Fort Bend County's values, principles, and legal requirements.

Acknowledgment of Policy Limitations

Fort Bend County acknowledges that the guidelines outlined in this document are not exhaustive. All policies within the County remain subject to revision at any time, with or without explicit mention in this document. This policy serves as a concise overview of AI usage in the County but may not encompass all current instances, applications, or guidelines in effect.

Glossary of Key Terms

Artificial Intelligence (AI): A machine-based system defined under 15 U.S.C. § 9401(3) that can make predictions, recommendations, or decisions based on human-defined objectives, influencing real or virtual environments. AI systems use machine- and human-based inputs, analyze environments, and use models to formulate actionable options.

Emerging Technologies Committee: A committee tasked with evaluating the use, benefits, risks, and mitigation strategies for emerging technologies within the County.

PHI (Protected Health Information): Data related to health status, provision of healthcare, or payment for healthcare that can be linked to an individual.

PII (Personally Identifiable Information): Information that can identify an individual, such as names, Social Security numbers, or biometric records.

Ownership: Refers to the rights Fort Bend County holds over data provided to and received from AI tools, prohibiting unauthorized use of copyrighted or proprietary materials.

Generative AI: AI systems capable of creating content such as text, images, or code based on input data.

Confidential Data: Sensitive information, such as PHI or PII, that is restricted from being provided to AI systems to protect privacy. Confidential Data also includes, but is not limited to, proprietary information, third-party intellectual property, copyrights, trademarks, financial information, and personal data of employees.

AI Inventory: A regularly updated report documenting all AI tools used and recommended by Fort Bend County.

Authorized Use: Strict adherence to laws, regulations, and policies governing the use of AI tools exclusively for official County activities.

Accuracy and Accountability: Employees are responsible for ensuring the accuracy of AI-generated content and for maintaining accountability for its use in official communications.

Data Minimization: Collecting and processing only essential data necessary for the function of Generative AI systems, avoiding unnecessary data to reduce privacy risks.

Prohibition of Sole Reliance: Ensures that human judgment is exercised alongside AI-generated insights and decisions are not based solely on AI outputs.

Prohibition of Harmful Activities: Restriction against using AI for activities that are illegal, unethical, or violate County policies.

Secure Development Practices: Ensuring that AI models and applications are built with secure coding methods, undergo rigorous testing, and are protected against vulnerabilities.

Third-Party Security Evaluation: Assessments conducted on third-party AI tools or services to ensure vendor security and compliance with County standards.

Discretionary Authority: The right of Fort Bend County to reject the use of AI by vendors if it does not meet County policies or standards.

Policy Limitations: Acknowledgment that the policy serves as a summary and may not encompass all guidelines or scenarios related to AI usage in the County.

Revision History

Change Initiator	Management Approver	Summary of Changes	Date	Revision Number
Emmanuel Effiong	Lee Morgan	Initial Version	10/31/2025	1.0