Black Hawk County Generative Artificial Intelligence Policy

Purpose

This policy outlines the principles, guidelines, and requirements for the responsible and ethical use of Artificial Intelligence (AI) within Black Hawk County. It is designed to ensure that AI technologies are used in a way that aligns with our values, respects human rights, and promotes accountability, fairness, and transparency.

Scope

This policy applies to all Black Hawk County employees, elected officials, contractors, vendors, and stakeholders involved in designing, procuring, deploying, or using AI tools. It covers all forms of AI interaction—text, voice, image, data feeds—and outputs including analytics, automated decisions, or reports. It also governs third-party AI systems that the county procures or uses, requiring compliance with relevant laws and ethical standards.

1. Definitions

- **Artificial Intelligence (AI)**: Technologies capable of simulating human intelligence, such as learning, reasoning, and problem-solving.
- **Bias**: Systematic unfairness or discrimination in AI outcomes caused by flawed data, algorithms, or assumptions.
- **Explainability**: The ability to understand and articulate how an AI system generates its output.
- **Fictitious Data**: Intentionally fabricated data mirroring the format of real data without revealing actual personal details.
- **Deidentified Data**: Data where personally identifiable information (PII) has been removed or replaced with non-reversible identifiers.
- **Encrypted Data**: Data transformed using cryptographic methods so that it cannot be accessed or understood without proper keys.
- **Protected health information (PHI)**: any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.
    - Ex. Full name, medical record number, diagnosis and medical condition, prescription info, billing and insurance info, etc.
- **Personal Identifiable Information (PII)**: any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
    - Ex. Full name, last four of social security number, birthdate, race, etc.

2. Tiered Approach to AI Usage

To balance innovation with compliance, AI use in Black Hawk County is governed by **tiers** based on data sensitivity, potential impact, and regulatory requirements. The following tier structure and associated guidance is required when using AI systems and tools:

Tier 1: Low-Risk / General Use

- **Permitted Tools**: Public-facing, generally available AI (e.g., ChatGPT, Co-Pilot, Gemini, etc.) or built-in AI features in software, used **only for non-sensitive tasks**.
- **Data Restrictions**: No personally identifiable information (PII), personal health information (PHI), Credit Card Information (PCI-DSS), or confidential data may be input.
- **Examples**: Brainstorming, summarizing public documents, drafting outlines, generating ideas.
- **Guidance**:
    - Employees may use these tools **without special approval**, provided they complete an AI awareness training course.
    - Any output is reviewed by the user for accuracy before official use.
    - Department Heads reserve the right to limit or revoke AI usage at their discretion.

Tier 2: Moderate-Risk / County-Licensed Use

- **Permitted Tools**: AI services with additional data-handling or enterprise security assurances (e.g., Microsoft 365 Copilot, Google Vertex AI) **under a County-licensed account**.
- **Data Restrictions**: Limited sensitive data, but **only** if the platform contractually prevents using the data to train public models. Deidentified, fictitious, or encrypted data is strongly recommended.
- **Examples**: Drafting certain internal documents, preliminary analysis involving limited or deidentified data.
- **Guidance**:
    - Requires an approved request to the IT Department and use of **licensed accounts** (no free trials or personal accounts).
    - Departments may be required to demonstrate intended use, benefits, and alignment with policy.
    - Any fully automated AI decision program is considered Tier 3.
    - Any moderate-risk AI usage must still comply with HIPAA, CJIS, PCI-DSS, or other relevant regulations.

Tier 3: High-Risk / Restricted Use

- **Permitted Tools**: AI solutions or models deployed **on-premises or in a secure, private cloud** managed by the County (or a vendor under strict contract).
- **Data Restrictions**: May involve regulated or highly sensitive data (e.g., PHI, law enforcement data), but **only** within systems explicitly designed and audited for compliance.
- **Examples**:
    - Sheriff's Office analyzing law-enforcement data (CJIS).
    - Public Health Department using PHI for analytics under HIPAA-compliant cloud infrastructure.

- **Guidance**:
    - Mandatory **risk assessment** and data protection review by IT and relevant compliance officers. Assessment includes 3rd party vendors who use AI.
    - **No external or public AI systems** can handle data at this level.
    - Ongoing audits, access logs, and compliance checks are required.

3. General Principles and Guidelines

3.1 Ethics and Responsible Use

- AI systems must prioritize fairness, accuracy, and respect for individual rights.
- They should not engage in discrimination or harm.
- **Human oversight** remains central for critical processes (hiring, financial decisions, public safety, medical diagnoses).

3.2 Transparency, Privacy & Security

- Relevant stakeholders should understand how AI systems produce outputs.
- Records generated or stored by AI vendors may be subject to public records requests.

3.3 Privacy and Security

- All AI applications must comply with **HIPAA, CJIS, PCI-DSS**, and other legal obligations and regulations.
- Sensitive data must be deidentified, encrypted, or replaced with fictitious data to safeguard privacy.

3.4 Inclusivity and Accessibility

- AI systems should avoid reinforcing societal biases and align with the County's anti-discrimination policy.
- They must be accessible to users of diverse abilities and backgrounds.

3.5 Data Use and Quality

- Use high-quality, representative datasets for AI model training and evaluation.
- Regularly evaluate systems to address data shifts and ensure continued reliability.

3.6 Environmental Impact

- The County recognizes that AI technologies have environmental impacts, including energy use and e-waste, and encourages departments to consider sustainability when selecting and operating AI systems.

3.7 Continuous Monitoring and Auditing

- Periodically audit AI systems for compliance, correctness, and unintended consequences.
- Have mechanisms to identify and correct errors or biases.

4. Prohibited Uses of AI

The organization explicitly prohibits the use of AI systems for the following purposes but is not limited to:

- **Surveillance** that violates privacy laws or ethical guidelines.
- **Discriminatory AI applications** (hiring, credit scoring, housing allocation).
- **Manipulative or deceptive content** (deepfakes, misinformation) without explicit consent.
- **Weaponization of AI** or any use causing physical or psychological harm.
- **Ingesting copyrighted material** into AI systems without proper authorization or licensing.
- Black Hawk County AI Committee reserves the right to adopt additional prohibited uses.

5. Compliance, Enforcement, and Training

5.1 Training and Awareness

- All employees must complete training on responsible AI usage.
- Resources will be available to understand emerging AI technologies and potential risks.

5.2 Reporting & Incident Management

- Any concerns or violations regarding the use of AI must be reported to the IT Department.
- Whistleblowers are protected against retaliation.
- In case of violations (ethical breaches, data leaks), the AI system may be suspended, investigated, and corrected. Severe or repeated violations may result in disciplinary action.

5.3 Enforcement

- Violations may result in disciplinary measures, up to and including termination, as outlined in the organization's disciplinary procedures. This includes negligent misuse or intentional misuse of AI technologies.

Review and Updates

This policy will be reviewed by the BHC AI Committee **every six months** (or as required) to address evolving legal, technological, or organizational changes. Revisions will be

communicated to all stakeholders to ensure ongoing alignment with best practices and regulations.