Van Buren County AI Usage Policy

3/6/25

1. Purpose

This policy establishes guidelines for the ethical and secure use of Artificial Intelligence (AI) technologies in Van Buren County operations. It aligns with existing policies, including the Personnel Handbook and Internet Security Policy, to ensure AI tools enhance service delivery while adhering to ethical, legal, and operational standards.

The Digital Information Department (DID) is responsible for managing AI systems throughout their entire lifecycle—development, deployment, maintenance, updates, and decommissioning. DID will report AI-related activities, progress, and performance to the AI Steering Committee regularly to ensure continuous oversight.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who use AI systems in their work with Van Buren County. It governs all AI-driven processes affecting decision-making, service delivery, or data processing.

3. Policy Guidelines

3.1 Ethical Standards

- **Transparency:** AI-generated decisions or outputs must be clearly labeled and explainable, especially in public-facing applications (refer to Personnel Handbook, Standards of Conduct Policy, Section 13; Internet Security Policy, Public Representations).
- **Human Accountability:** Users are ultimately responsible for the content and outcomes produced by AI systems. Human oversight is essential to ensure AI decisions are justifiable, align with the county's ethical standards, and meet public expectations. For AI systems impacting individual rights or freedoms, human oversight is mandatory to uphold accountability and ensure compliance with the Personnel Handbook's Standards of Conduct Policy.
- **Bias Mitigation:** AI systems must be monitored to minimize biases, ensuring compliance with the Equal Employment Opportunity Policy in the Personnel Handbook (Section 6).

3.2 Acceptable Use

- **Enhancement:** AI should enhance employee capabilities and improve efficiency.
- **Data Handling:** AI systems must process data in compliance with the Internet Security Policy, particularly its guidelines on Information Movement and Information Protection.
- **Tool Use:** AI tools must only be used for authorized purposes and must align with the county's ethical and operational standards (Personnel Handbook, Information Technology and Equipment Usage Policy, Section 24).
- **Privacy Compliance:** AI systems must adhere to privacy laws and policies, especially regarding sensitive data such as Social Security Numbers (refer to Personnel Handbook, Social Security Number Privacy Policy, Section 15).

3.3 Prohibited Use

- **Sensitive Data Restrictions:** AI systems must not process sensitive information (e.g., Criminal Justice Information, Personal Health Information) unless explicitly authorized. Any exceptions must be approved by both the DID and the Local Agency Security Officer (LASSO), ensuring compliance with CJIS requirements. A whitelist/blacklist approach will be maintained for approved AI tools.
- **Discriminatory Practices:** AI must not be used in ways that conflict with anti-discrimination or anti-harassment policies (Personnel Handbook, Sections 6-8).
- **Unauthorized Activities:** Employees are prohibited from using AI systems for personal gain or purposes that could create conflicts of interest (Personnel Handbook, Standards of Conduct Policy).

3.4 Compliance and Monitoring

- **Monitoring:** AI systems will be regularly monitored to ensure compliance with the Internet Security Policy's Compliance Monitoring section and adherence to county ethical standards (Personnel Handbook, Standards of Conduct Policy).
- **Incident Reporting:** Misuse or unethical deployment of AI systems must be reported in accordance with the Internet Security Policy's Reporting Security Problems section and the Personnel Handbook's Fraud and Abuse Policy (Section 10).
- **Training:** Employees using AI tools must complete training on AI ethics and security, supplementing existing training under the Personnel Handbook's Employee Development Policies. All employees must complete an AI Basics 101 course before gaining access to AI tools. Continuing education on AI will be required periodically to keep employees updated on evolving AI technologies and regulations.

4. Governance

- **AI Steering Committee:** A board-appointed body responsible for governing and overseeing all AI-related policies and activities, with more frequent oversight as needed.

- **AI Task Force:** A specialized technical committee tasked with evaluating potential AI solutions within individual departments.
- **Digital Information Department (DID):** Implements approved AI solutions, ensuring alignment with the Internet Security Policy and personnel practices outlined in the Personnel Handbook.

5. Metrics and Evaluation

The Digital Information Department will define and track metrics to evaluate AI system success, including:

- **Operational Efficiency:** Metrics such as time savings and task automation rates.
- **Financial Impact:** Measures such as cost reductions or savings.
- **User Satisfaction:** Feedback from employees and citizens.

These metrics will be reviewed quarterly, with a full evaluation reported regularly to the AI Steering Committee. The DID will also establish performance evaluation timelines to ensure regular assessments throughout the lifecycle of AI systems.

6. Policy Review

This policy will be reviewed regularly to reflect technological advancements and legal changes. Reviews will include cross-references to updates in the Internet Security Policy and Personnel Handbook (Section 1: Adoption and Administration of Policies).

7. Enforcement

Violations of this policy will result in disciplinary action per the Personnel Handbook's Disciplinary Policies and the Internet Security Policy's Disciplinary Process. Severe violations may lead to termination or legal action.