RESOLUTION NO. 130-2026

A RESOLUTION ADOPTING THE "CYBERSECURITY & ARTIFICIAL INTELLIGENCE USE POLICY" FOR THE TOWN OF OAK GROVE, ARKANSAS; AND FOR OTHER PURPOSES.

WHEREAS, the State of Arkansas enacted **Act 489 of 2025**, establishing statewide cybersecurity standards and requiring public entities to implement cybersecurity policies, incident reporting procedures, and employee training; and

WHEREAS, the State of Arkansas enacted **Act 848 of 2025**, originating from House Bill 1958, requiring all public entities to adopt a policy governing the authorized use of artificial intelligence (AI) and automated decision tools; and

WHEREAS, the Town of Oak Grove recognizes the importance of protecting municipal systems, resident data, and public information from cybersecurity threats, while ensuring responsible, transparent, and ethical use of artificial intelligence; and

WHEREAS, the Town Council desires to formally adopt the **Cybersecurity & Artificial Intelligence Use Policy**, attached hereto as *Exhibit A*, to ensure compliance with state law and to establish clear standards for employees, officials, contractors, and volunteers.

NOW, THEREFORE, BE IT RESOLVED BY THE TOWN COUNCIL OF THE TOWN OF OAK GROVE, ARKANSAS:

SECTION 1. ADOPTION OF POLICY.

The Town Council hereby adopts the **Cybersecurity & Artificial Intelligence Use Policy**, attached as *Exhibit A* and incorporated by reference as if fully set forth herein.

SECTION 2. IMPLEMENTATION.

Town employees, elected officials, contractors, and volunteers shall comply with the policy. The Mayor and Secretary/Treasurer are authorized to implement and enforce the policy and to ensure required training is completed.

SECTION 3. UPDATES & REVIEW.

The policy shall be reviewed annually and updated as needed to remain compliant with Arkansas law, state cybersecurity directives, and best practices.

SECTION 4. EFFECTIVE DATE.

This resolution shall be effective immediately upon its passage and approval.

PASSED AND APPROVED this 6 day of January, 2026.

ATTEST:

Mayor

Secretary/Treasurer

APPROVED BY COUNCIL:

Gary Gray, Aaron Curtis, Terry Hutchison

CYBERSECURITY & ARTIFICIAL INTELLIGENCE USE POLICY
Adopted by: Town of Oak Grove
Effective Date: January 6, 2026

---

1. Purpose

This policy establishes cybersecurity, data protection, and artificial intelligence (AI) governance requirements for **Town of Oak Grove**, ensuring compliance with:

- **Act 489 of 2025 – Arkansas Cybersecurity Act of 2025**, which centralizes cybersecurity oversight and requires state and local entities to follow statewide cybersecurity standards.
- **Act 848 of 2025 – Public Entity AI Use Policy Requirements**, mandating that all Arkansas public entities adopt a policy governing the authorized use of AI and automated decision tools.

This policy protects residents, employees, systems, and data while enabling responsible, transparent, and ethical use of technology.

---

2. Scope

This policy applies to:

- All employees, contractors, elected officials, volunteers, and temporary staff.
- All information systems, networks, devices, applications, and data owned or operated by the entity.
- All uses of AI systems, automated decision tools, and machine-based analytics.

---

3. Definitions

3.1 Cybersecurity
As defined in Act 489, cybersecurity includes the protection of systems, networks, and data from unauthorized access, attacks, or damage.

3.2 Artificial Intelligence (AI)
As defined in Act 848, AI is a machine-based system capable of making predictions, recommendations, or decisions based on human-defined objectives.

3.3 Automated Decision Tool
A system designed to make or significantly influence decisions affecting rights, services, or access to public benefits.

3.4 Human Final Decision Authority
Act 848 requires that **all final decisions remain with a human employee**, not an AI system.

---

4. Cybersecurity Governance (Act 489 Compliance)

4.1 Alignment with the State Cybersecurity Office

Town of Oak Grove, AR shall follow all standards, directives, and best practices issued by the **Arkansas State Cybersecurity Office** and the **State Information Security Officer**, as required by Act 489.

4.2 Security Controls

The entity shall implement:

- Multi-factor authentication
- Network monitoring and intrusion detection
- Regular patching and updates
- Access controls based on least privilege
- Data encryption for sensitive information
- Secure configuration baselines

4.3 Incident Response

The entity shall:

- Maintain an incident response plan aligned with state guidance
- Report cybersecurity incidents to the State Cybersecurity Office as required by Act 489
- Document all incidents and corrective actions

4.4 Employee Training

Annual cybersecurity training is mandatory for all employees and contractors.

4.5 Third-Party Vendors

Vendors must comply with state cybersecurity standards and sign data-protection agreements.

---

5. Authorized Use of Artificial Intelligence (Act 848 Compliance)

5.1 Human Oversight Requirement

AI may assist with analysis, drafting, or recommendations, but **a human employee must review, approve, and remain responsible for all final decisions**.

5.2 Transparency

The entity shall:

- Publicly post this AI policy on its website, as required by Act 848
- Disclose when AI tools are used in public-facing services or communications

5.3 Prohibited Uses

AI may **not** be used for:

- Fully automated decision-making without human review
- Decisions affecting legal rights, benefits, or access to public services
- Surveillance or monitoring without explicit legal authority
- Any use that violates privacy, civil rights, or state/federal law

5.4 Approved Uses

AI may be used for:

- Drafting documents, notices, or communications
- Data analysis, forecasting, and administrative efficiency
- Customer service assistance (with human review)
- Internal workflow automation

5.5 Accuracy & Bias Mitigation

Employees must:

- Verify AI-generated content for accuracy
- Check for bias, discrimination, or harmful outputs
- Document significant uses of AI in decision-making processes

5.6 Employee Training

Act 848 requires training programs for employees using AI tools.
Training shall include:

- Proper use of AI systems
- Risks, limitations, and bias awareness
- Privacy and data-handling requirements

---

6. Data Privacy & Protection

- AI tools may not be used to process sensitive personal data unless authorized by law.
- No confidential, restricted, or legally protected information may be entered into external AI systems without approval.
- All data used in AI systems must comply with state and federal privacy laws.

---

7. Documentation & Recordkeeping

The entity shall maintain:

- A list of all approved AI tools
- Documentation of AI use cases
- Records of human review for decisions influenced by AI
- Cybersecurity incident logs
- Annual training records

---

8. Policy Review & Updates

This policy shall be reviewed **annually** or sooner if:

- State cybersecurity standards change
- New AI tools are adopted
- Laws or regulations are updated

Updates must be approved by the governing body.

---

9. Enforcement

Violations of this policy may result in:

- Revocation of system access
- Disciplinary action
- Contract termination for vendors
- Reporting to state authorities when required by law

---

10. Adoption

Approved by Council Members: Terry Hutchison
Gary Gray
Aaron Curtis

Date: January 6, 2026

Mayor

Secretary/Treasurer

TOWN OF OAK GROVE, ARKANSAS
INCIDENT RESPONSE PLAN (IRP)

Adopted: January 6, 2026
Companion to the Cybersecurity Policy (Act 489 Compliance)

1. Purpose

This Incident Response Plan establishes the procedures the Town of Oak Grove will follow to identify, contain, report, and recover from cybersecurity incidents. It ensures compliance with **Arkansas Act 489 of 2025**, which requires public entities to follow statewide cybersecurity standards and report incidents to the Arkansas State Cybersecurity Office.

2. Scope

This plan applies to:

- All Town employees, elected officials, contractors, and volunteers
- All Town-owned or Town-managed systems, networks, devices, and data
- Any suspected or confirmed cybersecurity incident

3. Definitions

- **Cybersecurity Incident:** Any attempted or actual unauthorized access, disruption, loss, or compromise of Town systems or data.
- **Breach:** A confirmed incident resulting in unauthorized access to sensitive or protected information.
- **Incident Response Team (IRT):** The individuals responsible for managing and resolving incidents.

4. Incident Response Team (IRT)

Because Oak Grove is a small municipality, the IRT is streamlined and role-based. Each role may be filled by the person currently holding that office or their designee.

4.1 Primary Roles

Role	Responsibility
Mayor or Designee	Serves as Incident Commander; authorizes major actions, external notifications, and coordination with the Arkansas State Cybersecurity Office.
Secretary/Treasurer	Maintains incident documentation, logs, timelines, and communication records; assists with internal notifications; tracks costs and financial impacts.
Recorder	Manages records retention related to the incident; ensures compliance with FOIA, documentation requirements, and preservation of digital evidence.
IT Support / Contractor	Leads technical investigation, containment, eradication, and system restoration; provides technical reports and recommendations.
Department Heads	Identify operational impacts, assist with staff communication, and implement department-level containment or recovery steps.

4.2 When to Activate the IRT

The IRT is activated for any suspected or confirmed cybersecurity incident, including but not limited to:

- Phishing attempts or suspicious emails
- Malware or ransomware detection
- Unauthorized access attempts
- Lost or stolen devices
- System outages with unknown cause
- Any event involving sensitive or protected data

5. Incident Response Phases

Phase 1 — Identification

Employees must immediately report:

- Suspicious emails
- Unexpected system behavior
- Unauthorized login alerts
- Lost or stolen devices
- Files or systems that appear altered

Reports go to:

- **Supervisor**, and
- **Recorder/Treasurer**, who notifies the Mayor and IT support

The IRT determines:

- What happened
- When it happened
- Which systems or data are affected
- Whether the incident is ongoing

Phase 2 — Containment

The goal is to stop the incident from spreading. Actions may include:

- Disconnecting affected devices from the network
- Disabling compromised accounts
- Blocking malicious IP addresses
- Stopping unauthorized processes
- Changing passwords
- Restricting access to affected systems

Short-term containment is followed by long-term containment, such as:

- Applying patches
- Updating firewall rules
- Strengthening authentication

Phase 3 — Eradication

The IRT removes the cause of the incident. This may include:

- Removing malware
- Deleting unauthorized accounts
- Rebuilding compromised systems

- Applying security updates
- Reviewing logs for hidden persistence

Phase 4 — Recovery

The Town restores normal operations safely. Actions include:

- Restoring systems from clean backups
- Monitoring systems for unusual activity
- Validating that services are functioning normally
- Re-enabling accounts with updated credentials
- Confirming that vulnerabilities have been addressed

Recovery timelines depend on severity.

Phase 5 — Reporting (Act 489 Requirement)

Under Act 489, the Town must report cybersecurity incidents to the **Arkansas State Cybersecurity Office** when:

- Sensitive data may be compromised
- Systems are significantly disrupted
- Ransomware or malware is involved
- Unauthorized access is confirmed

The Mayor or designee coordinates the report.

If residents' personal information is affected, the Town will provide legally required notifications.

Phase 6 — Post-Incident Review

Within 10 business days, the IRT conducts a review to document:

- What happened
- How it happened
- How long it lasted
- What data or systems were affected
- What actions were taken
- What improvements are needed

A written After-Action Report (AAR) is filed and retained.

6. Employee Responsibilities

All employees must:

- Complete annual cybersecurity training
- Report incidents immediately
- Follow password and MFA requirements
- Avoid using personal devices for Town business unless authorized
- Never attempt to "fix" an incident themselves

7. Vendor Responsibilities

Vendors with access to Town systems must:

- Notify the Town immediately of any breach
- Cooperate fully with investigations
- Follow Town and state cybersecurity standards

8. Documentation Requirements

The Recorder/Treasurer maintains:

- Incident logs
- After-Action Reports
- Communications with state authorities
- Evidence collected during investigations
- Training records

9. Plan Review & Updates

This Incident Response Plan shall be reviewed **annually** or sooner if:

- State cybersecurity guidance changes
- New systems or technologies are adopted
- An incident reveals gaps in the plan

Updates must be approved by the Mayor and/or Town Council depending on adoption method.