**DIS at a Glance**

Premier IT Products & Solutions Provider
Serving The Following Entities in Arkansas’s Public Sector:

- State Agencies
- Boards
- Commissions
- K-12 Schools
- Higher Education
- Public Safety
- County Government
- City Government

$80 Million
IT Products & Solutions

1,500 +
Governmental Sites Served

24/7/365
Monitoring & Support

**VALUES**

Technology Leadership | Customer Service | Quality Results | Efficiency

- Remote Field Support
- 24/7/365 Call Center
- Desktop Support
- IT Planning & Consulting

**VALUE**

DIS negotiates with vendors to leverage the state’s buying power

**SERVICES**

DIS is the engine that keeps public systems operational

- Internet Connectivity
- Secure Data Center Hosting
- Virtual Private Cloud
- Data Analytics
- Voice over Internet Protocol
- Voicemail & Email
- Audio & Video Conferencing
- Tape, Data Storage & Backup
- Network Security
- Windows Desktop Support
- Application Development
- Cybersecurity
- Business Continuity
- Disaster Planning & Recovery
- Systems Integration
- Project Management

Arkansas Department of Information Systems

EMPOWERING THE CITIZENS OF ARKANSAS THROUGH TECHNOLOGY
FACTS
An enterprise agreement with Microsoft consolidated all licenses procured by the state into a single agreement.

The state’s annual spend with Microsoft is going up, but this agreement is bringing the overall cost of the state’s IT investment down.

Reduced or Eliminated Costs
- Implementation costs
- Anti-virus solution cost
- MDM solution cost
- MFA solution cost
- Cost of IT computing
- Man-Hour costs

Operational & Security Benefits
The average cost of a data breach in the U.S. for each lost or stolen record is $141 (2017). A single data breach cost one state $27 million. The enhanced protections integrated into the Microsoft solutions offer an extra layer of security to protect state computers and email accounts from phishing, malware, ransonware and other malicious activity.

Core components hosted in Government Cloud
- Data classification to enable safe sharing of sensitive data
- Visibility & control of shared data
- Simplified IT management & operations
- Upgrades, patches & infrastructure maintenance: Eliminated
- Centrally managed single sign-on across devices
- Comprehensive intelligent protection against today’s advanced attacks
- Visibility & control over shared data to reduce the risk of a data breach