

# INFORMATION TECHNOLOGY MANAGED SERVICES AGREEMENT

This Information Technology Managed Services Agreement (“Agreement”) is entered into as of \_\_\_\_\_ (“Effective Date”), by and between:

**Customer:** \_\_\_\_\_, a political subdivision of the State of Texas (“Customer”), with offices located at \_\_\_\_\_;

and

**Service Provider:** \_\_\_\_\_, a  
\_\_\_\_\_, with offices located at  
\_\_\_\_\_ (“Provider”).

Collectively referred to as the “Parties.”

---

## 1. PURPOSE

Provider shall furnish managed information technology services, technical support, cybersecurity services, consulting, and related services for Customer’s information technology environment in accordance with this Agreement.

---

## 2. TERM

The initial term of this Agreement shall begin on the Effective Date and continue for three (3) years unless terminated earlier under this Agreement.

Customer may renew this Agreement for up to two (2) additional one-year terms by written agreement.

---

## 3. SCOPE OF SERVICES

Provider shall perform the following services:

### Managed Infrastructure

- Server administration
- Virtual server management
- Network monitoring

- Firewall administration
- Wireless infrastructure management
- VPN management
- Microsoft Active Directory administration
- Microsoft 365 administration
- Cloud services management
- DNS management
- DHCP management

### Endpoint Management

- Desktop support
- Laptop support
- Mobile device support
- Patch management
- Operating system upgrades
- Endpoint security
- Antivirus management
- Endpoint Detection and Response (EDR)

### Help Desk

Provider shall provide:

- Unlimited remote help desk
- Onsite support as required
- Ticket management
- User administration
- Password resets
- Software troubleshooting
- Printer support

Hours:

Monday through Friday

7:00 AM – 6:00 PM Central Time

Emergency support available 24x7.

---

## 4. CYBERSECURITY SERVICES

Provider shall provide:

- Security monitoring
  - Security incident response
  - Vulnerability scanning
  - Multi-factor authentication management
  - Security awareness training
  - Email security
  - DNS filtering
  - Backup monitoring
  - Disaster recovery planning
  - Security reporting
- 

## 5. BACKUP SERVICES

Provider shall:

- Monitor backup jobs daily
  - Perform quarterly restore testing
  - Maintain off-site backup copies
  - Notify Customer of backup failures within one business day
- 

## 6. SERVICE LEVEL AGREEMENT (SLA)

### Priority 1 – Critical

Examples:

- Network outage
- Server failure
- Ransomware
- Internet outage affecting government operations

Response:

Within 30 minutes

Target Resolution:

Four (4) hours

---

## Priority 2 – High

Examples:

- Multiple users affected
- Application unavailable
- Major printer outage

Response:

One (1) hour

Resolution:

Eight (8) business hours

---

## Priority 3 – Medium

Examples:

- Single user issue
- Software problem

Response:

Four (4) business hours

Resolution:

Two (2) business days

---

## Priority 4 – Low

Examples:

- Information request
- New workstation
- Routine changes

Response:

One (1) business day

Resolution:

Five (5) business days

---

## 7. PROVIDER RESPONSIBILITIES

Provider shall:

- Maintain qualified personnel.
  - Follow industry best practices.
  - Maintain security controls.
  - Document Customer systems.
  - Maintain confidentiality.
  - Notify Customer of security incidents immediately.
  - Maintain professional liability insurance.
  - Perform services in accordance with applicable laws.
- 

## 8. CUSTOMER RESPONSIBILITIES

Customer shall:

- Provide system access.
  - Designate an IT liaison.
  - Maintain software licensing.
  - Provide accurate asset information.
  - Promptly report problems.
  - Maintain physical security of facilities.
- 

## 9. CHANGE MANAGEMENT

Changes affecting production systems shall require written approval by Customer unless necessary to mitigate an active cybersecurity incident or prevent imminent service interruption.

Emergency changes shall be documented within one business day.

---

## 10. FEES

Customer shall pay Provider as follows:

Monthly Managed Services Fee:

\$\_\_\_\_\_ per month.

Additional Services:

\$\_\_\_\_\_ per hour.

Projects shall be separately quoted unless specifically included.

Invoices are due within thirty (30) days.

---

## 11. PUBLIC INFORMATION

Provider acknowledges that Customer is subject to the Texas Public Information Act.

Provider shall:

- Cooperate with records requests.
  - Clearly identify confidential proprietary information.
  - Understand that Customer makes the final determination regarding disclosure unless otherwise required by law.
- 

## 12. DATA OWNERSHIP

All Customer data remains the exclusive property of Customer.

Provider acquires no ownership rights.

Upon termination, Provider shall return all Customer data in a mutually agreed electronic format.

---

## 13. CONFIDENTIALITY

Provider shall not disclose confidential information except:

- with Customer authorization;
- as required by law; or
- pursuant to court order.

Confidentiality obligations survive termination for five (5) years.

---

## 14. CYBER INCIDENTS

Provider shall notify Customer within one (1) hour after discovering any cybersecurity incident affecting Customer systems.

Provider shall:

- assist with containment;
  - preserve evidence;
  - cooperate with law enforcement when requested by Customer;
  - provide written incident reports.
- 

## 15. COMPLIANCE

Provider shall comply with applicable federal and Texas laws, including those governing data security, privacy, accessibility, licensing, and records retention applicable to local governments.

---

## 16. INSURANCE

Provider shall maintain:

Commercial General Liability:

\$1,000,000 per occurrence

Professional Liability (Errors & Omissions):

\$2,000,000

Cyber Liability:

\$5,000,000

Workers Compensation:

As required by Texas law

Certificates of insurance shall be provided upon request.

---

## 17. LIMITATION OF LIABILITY

Except for liability arising from gross negligence, willful misconduct, breach of confidentiality, infringement of intellectual property rights, or obligations relating to data security expressly assumed under this Agreement, neither Party shall be liable for indirect, incidental, consequential, special, or punitive damages to the extent permitted by law.

Nothing in this Agreement shall be construed as a waiver of Customer's governmental or sovereign immunity or any defenses available under Texas law.

---

## 18. TERMINATION

Customer may terminate:

- for convenience upon sixty (60) days written notice;
- immediately for material breach if not cured within thirty (30) days;
- immediately for cybersecurity risks that materially threaten Customer operations.

Upon termination Provider shall:

- cooperate in transition;
  - return all passwords;
  - return all documentation;
  - return all backups;
  - remove Provider-owned software where appropriate;
  - certify deletion of Customer data retained by Provider, except where retention is required by law.
- 

## 19. DISPUTE RESOLUTION

The Parties shall first attempt good-faith negotiations.

Venue shall lie in the county in which Customer is located, unless otherwise required by applicable law.

This Agreement shall be governed by the laws of the State of Texas.

---

## 20. FORCE MAJEURE

Neither Party shall be liable for delays caused by events beyond reasonable control, excluding obligations related to data security where reasonable preventive measures were required.

---

## 21. SUBCONTRACTORS

Provider shall remain responsible for the acts and omissions of its subcontractors.

Subcontractors having access to Customer data must be bound by confidentiality and security obligations substantially similar to those in this Agreement.

---

## 22. PERSONNEL

Provider shall ensure personnel:

- pass criminal background checks appropriate for access to government facilities or information;
  - complete cybersecurity awareness training annually;
  - comply with Customer security policies while on Customer premises or systems.
- 

## 23. BUSINESS CONTINUITY

Provider shall maintain a documented business continuity and disaster recovery plan and make a summary available to Customer upon request.

---

## 24. AUDIT RIGHTS

Customer may audit Provider's compliance with this Agreement upon reasonable notice, including review of security controls, service reports, and records related to services performed for Customer, subject to reasonable confidentiality protections.

---

## 25. NOTICES

All notices shall be in writing and delivered by certified mail, recognized overnight courier, or electronic mail with confirmation of receipt to the addresses designated by each Party.

---

## 26. ENTIRE AGREEMENT

This Agreement, including all exhibits and amendments, constitutes the entire agreement between the Parties and supersedes all prior discussions and understandings relating to its subject matter.

---

## 27. SIGNATURES

### **CUSTOMER**

Name:

Title:

Signature:

Date:

---

### **SERVICE PROVIDER**

Name:

Title:

Signature:

Date:

---

## EXHIBIT A – COVERED EQUIPMENT

(To be completed.)

---

## EXHIBIT B – PRICING

(To be completed.)

---

## EXHIBIT C – SERVICE LEVEL AGREEMENT

(Incorporated by reference.)

---

## EXHIBIT D – CYBERSECURITY REQUIREMENTS

- Multi-factor authentication
- Endpoint Detection and Response (EDR)
- Security Information and Event Management (SIEM), if applicable
- Encryption of data in transit and at rest where appropriate
- Quarterly vulnerability assessments
- Annual penetration testing (if included in scope)
- Annual disaster recovery testing
- Secure password and privileged access management
- Incident response procedures and escalation contacts