DWD
TECHNOLOGY GROUP

Managed IT Security Services

Protect Your Company & Data from Cybersecurity Threats

You have invested in your IT infrastructure and rely on its security, performance, and reliability. DWD's managed IT security services ensures you have a qualified team protecting this critical asset.

OVERVIEW

Managed IT Security Services have become a popular option for companies determined to stay on top of security risks by leveraging others' expertise.

With DWD's managed IT security services, you leverage the knowledge and experience of IT experts who possess a thorough understanding of networks, server backups, patch management, network monitoring, network security and more.

We seek to become an integral partner in protecting and supporting your business, as we continue to do for so many other businesses in Northeast Indiana.

BENEFITS OF MANAGED IT SECURITY SERVICES

- Minimize the costs to protect your business and data
- Gain access to unique cybersecurity expertise and tools
- Automatic detection and resolution of vulnerabilities
- Advanced malware threat monitoring & expertise
- Return your IT teams focus to your business goals
- Better manage Risk and Compliance

Managed IT Security Plans

We offer customized Managed IT Security plans to best fit the needs of your company. Select products/ services from the tiered options below to build a Managed IT security program to protect your business.

Product / Service	Basic (Minimum)	Preferred (Recommended)	Premium
Backup	✓	✓	✓
Disaster Recovery	✓	✓	✓
Password Guidance	✓	✓	✓
Antivirus/Antimalware	✓	✓	✓
Firewalls	✓	✓	✓
Switches	✓	✓	✓
Secure Wireless Networks	✓	✓	✓
Secure Remote Access	✓	✓	✓
Anti-spam	✓	✓	✓
Network Vulnerability Scanning		✓	✓
Network Security Assessments		✓	✓
Work from Home Security		✓	✓
Virtual Private Networks		✓	✓
Firewall Maintenance		✓	✓
Microsoft OS and Application Patching (Servers & Workstations)		✓	✓
Multifactor Authentication		✓	✓
Intrusion Prevention & Detection		✓	✓
Business Continuity		✓	✓
Cloud Delivered Enterprise Security		✓	✓
Security Awareness Training		✓	✓
Cloud Continuity			✓
Mobile Device Management			✓
24/7 Security Endpoint Threat Detection, Response and Remediation			✓
Fully Managed SIEM			✓
Dark Web Monitoring			✓
Email Encryption			✓

DWD TECHNOLOGY GROUP
9921 Dupont Circle Drive West, Suite 300, Fort Wayne, IN 46825
260.423.2414 • 800.232.8913
www.dwdtechgroup.com

Full Description of Product/Service Offerings

Backup - A copy of data stored elsewhere.

Disaster Recovery - Regaining access to programs and data following a disaster.

Password Guidance - Current best practices for creating and changing passwords.

Antivirus/Antimalware - Scan, detect and remove or quarantine malware from your computer.

Firewalls - The main entry and exit point for traffic to/from your network. Rules are set for what to let in and out.

Switches - At the simplest level, connect multiple devices on your network. Higher-end units can perform functions similar to a router.

Secure Wireless Networks - Current best practices for securing your wireless communications. This includes system types, broadcasting, channels, password management, whitelisting, and URL Filtering.

Secure Remote Access - Current best practices for allowing users to access the company network while offsite.

Antispam - System for blocking unwanted, and possibly malicious, emails.

Network Vulnerability Scans -Detect and classify network weaknesses by remotely scanning for open, vulnerable ports.

Network/Security Assessments - Can vary in detail from brief overview of network layout to capturing every device and every point of entry on a network. Results presented in a report and explained to client.

Work From Home Security - Current best practices for configuring remote access to company resources. Typically deals with virtual private networks, multi factor authentication and remote device scans to verify compliance.

Virtual Private Networks - A secure connection to another network.

Firewall Maintenance - Management of all applicable updates to a firewall: firmware, security data, service packs.

Microsoft OS and Application Patching on selected servers and workstations - Management of all applicable updates to a server or workstation, mainly Service Packs.

Multifactor Authentication - Requires a user to present two or more forms of identification; password, text to phone, USB device.

Intrusion Prevention & Detection - A system that detects existing malware (Detection) and proactively blocks attacks (Prevention).

Business Continuity - Ensure that a business can continue operations shortly following a disaster.

Cloud Delivered Enterprise Security - A first line of defense against cyber security threats. Often includes URL filtering.

Secure Network Design Services - Current best practices for securing endpoints, infrastructure and cloud access to company resources.

Security Awareness Training - Providing education for your staff on different threats to your information and often includes unannounced phishing emails to test their understanding.

Cloud Continuity - A complete backup of your computer stored in the cloud.

Mobile Device Management - Manage, monitor and secure mobile devices for employees. Most often provides for ways to lock or wipe sensitive data in case of loss or theft.

24/7 Security Endpoint Threat Detection, Response & Remediation - AI powered agent applied to computers and servers that provides detection and response to attacks and with some services the ability to roll back to a previous good state.

Fully Managed SIEM - A team of experts monitors your Security Incident and Event Management logs. Overwhelming for all but the largest companies.

Dark Web Monitoring - Allows you to be notified if identity information for you is found online.

Email Encryption - Email transmitted in a way that only the sender and receiver can read the message.

DWD TECHNOLOGY GROUP
9921 Dupont Circle Drive West, Suite 300, Fort Wayne, IN 46825
260.423.2414 • 800.232.8913
www.dwdtechgroup.com