WARNER TELECOMM

Enterprise Technology Management

Security Posture Overview

WARNER TELECOMM
Enterprise Technology Management

Our Assurance to You

At Warner Telecomm, the security of our clients' data and systems is our top priority. We have implemented a robust security posture that encompasses a wide range of features designed to protect against evolving threats. Our comprehensive approach ensures that every aspect of our operations, from network access to data storage, is fortified with the latest in security technology and best practices. This document provides an overview of the key security measures in place to safeguard your business, ensuring continuous protection and peace of mind.

Warner Security Posture Overview

24/7 NOC Support on Company-Provided Equipment

Workstation and Server Patching: Continuous updates to ensure systems are protected against vulnerabilities. Security Information and Event Management (SIEM): Centralized logging and analysis of security events for real-time threat detection. Monitoring: Comprehensive oversight of all network activities to detect and respond to potential threats. End User Device and Service Monitoring for Anti-Virus and Anti-Malware: Constant surveillance of devices to ensure they are free from malicious software.

US-Based Dual Disaster Recovery with Physical Access Security Restrictions

Dual Disaster Recovery: Two geographically distinct locations ensure that data is recoverable in the event of a disaster. Physical Access Security: Strict access controls at data centers to protect against unauthorized entry.

Cyber Insurance

Provides financial protection against losses due to cyber incidents, including data breaches and business interruptions.

WARNER TELECOMM
Enterprise Technology Management

WARNER TELECOMM
Enterprise Technology Management

Warner Security Posture Overview Cont.

Two-Factor Authentication (2FA)
Enhances security by requiring two forms of identification before granting access to systems, ensuring that only authorized users can log in.

Company-Owned Equipment with VPN Requirements
All connected equipment is company-owned, ensuring standardized security measures. A VPN connection is required to access the network, providing an additional layer of encryption and security.

Credential-Based Access
Users must adhere to strict password and account security protocols, ensuring that access is only granted to authorized personnel.

WARNER TELECOMM
Enterprise Technology Management

Warner Security Posture Overview Cont.

Data Stored in SOC II Compliant Data Center
All data is stored in facilities that meet SOC II standards, guaranteeing the highest levels of data security and compliance.

SOC I type II
Certified by the American Institute of Certified Public Accountants (AICPA), attests that our controls and processes meet rigorous industry requirements, ensuring reliable and compliant service delivery for our valued customers.

FileCloud Service for Secure Information Sharing
A secure platform for sharing and storing information, ensuring that sensitive data is protected during transfer and at rest.

Incident Response Team
A dedicated team available to respond to and mitigate the effects of security incidents, ensuring quick recovery and minimal impact.

WARNER TELECOMM
Enterprise Technology Management

Warner Security Posture Overview Cont.

- **Data Retention and Destruction Planning** - Comprehensive policies for retaining data only as long as necessary and securely destroying it when it is no longer needed.
- **Defined Change Management Process** - A structured approach to managing changes in the IT environment, reducing the risk of security breaches during transitions.
- **Background Checks and Drug Screening for All Employees** - Ensures that all employees with access to sensitive information have undergone thorough vetting.
- **Annual Penetration Tests** - Regular testing of security measures to identify and address vulnerabilities, ensuring ongoing protection.

WARNER TELECOMM
Enterprise Technology Management

Warner Security Posture Overview Cont.

- **Dual Redundancy**

Redundant systems and processes in place to ensure continuous operation and data availability even in the event of a failure.

- **Mobile Device Management (MDM)**

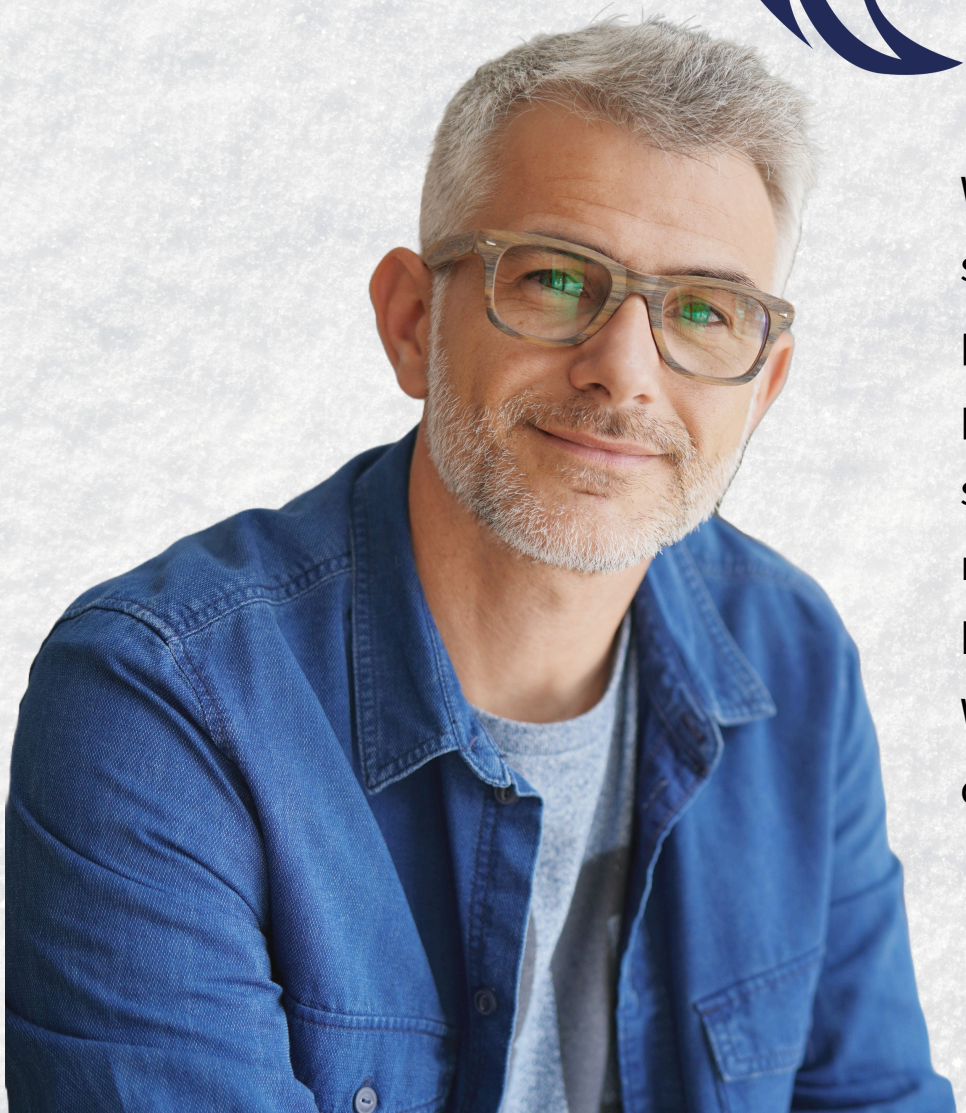
Secure management of mobile devices to protect against threats and ensure compliance with company policies.

- **Threat Detection**

Advanced threat detection systems actively monitor for suspicious activities, providing early warnings to prevent potential breaches.

"This comprehensive suite of security features ensures that your organization's data and systems are protected with the highest level of security, ensuring peace of mind and continuous operations".

WARNER
TELECOMM
Enterprise Technology Management



Warner Telecomm is committed to maintaining the highest standards of security for our clients. Our extensive security posture, which includes advanced technologies, stringent policies, and dedicated support, ensures that your data and systems are continuously protected. By investing in these robust measures, we provide a secure environment that allows your business to operate confidently in today's digital landscape. With Warner Telecomm, you can trust that your security is in capable hands.

For more information contact us at:
412-362-9000 - wtlcom.com