

Robocall Mitigation Program

Pursuant to the rules of the Federal Communications Commission, including 47 CFR Section 64.6305, CybertronIT has implemented the following Robocall Mitigation Program.

CybertronIT provides PBX installation, configuration, maintenance, and technical support services, including support for 3CX phone systems. CybertronIT does not originate, terminate, or transmit calls to the public switched telephone network (PSTN), and does not provide SIP trunking, DIDs, or telecommunications carrier services.

All voice traffic is transmitted through third-party voice service providers selected and contracted directly by customers. Those providers are responsible for call authentication, including STIR/SHAKEN implementation, and for compliance with applicable FCC robocall mitigation requirements.

CybertronIT's mitigation role is limited to the PBX systems it configures or manages. CybertronIT does not actively monitor customer calls, call content, live call activity, or customer call detail records unless specifically engaged to review an issue. CybertronIT can only review system alerts, security notifications, logs, or other information made available by 3CX, the customer, or the customer's voice service provider.

CybertronIT implements reasonable PBX security controls intended to reduce the risk of unauthorized calling or PBX compromise, including:

1. Deployment and maintenance of supported, current versions of 3CX where CybertronIT is responsible for PBX management.
2. Use of strong authentication controls, including long, complex passwords for applicable 3CX administrative, extension, and system accounts.
3. Requirement of multi-factor authentication for administrative access where supported and applicable.
4. Configuration of 3CX security features, access restrictions, firewall guidance, and intrusion prevention controls where appropriate.
5. Review of 3CX-generated alerts, notifications, or security events that are available to CybertronIT.
6. Assistance with investigation and remediation when a customer, 3CX, or a voice service provider identifies suspected fraud, compromise, abnormal call activity, or illegal robocalling.
7. Implementation of reasonable response actions where technically available, which may include disabling affected extensions, changing credentials, restricting outbound dialing, modifying PBX access controls, or coordinating with the customer's voice service provider.

CybertronIT requires customers to remain responsible for all telecommunications activity conducted through their phone systems and for compliance with applicable laws, including the Telephone Consumer Protection Act and the Truth in Caller ID Act.

In the event of suspected illegal robocalling or PBX compromise, CybertronIT will take reasonable steps within its technical role to help mitigate further activity and will cooperate with the customer, the customer-selected voice service provider, and lawful traceback or investigative requests, including those coordinated through the U.S. Telecom Industry Traceback Group.

CybertronIT maintains relevant PBX configuration records, support records, and available system logs to the extent reasonably accessible and necessary to support investigation and mitigation efforts.

This program is designed to reduce the risk of illegal robocalls while maintaining CybertronIT's role as a systems integrator and technical service provider, not a telecommunications carrier or voice service provider.