Headand Communications Security Policy

Effective Date: 07/25/2024

Security and privacy of your communications are our highest priority. As a managed Internet Telephony Service Provider, we take a proactive, layered approach to safeguard your voice and data services from evolving cyber threats.

Our Security Practices

1. Network Security

- All voice traffic is encrypted using TLS and SRTP to prevent interception and tampering.
- Firewalls and intrusion detection/prevention systems (IDS/IPS) guard our infrastructure 24/7.
- DDoS protection is continuously in place to ensure service availability.

2. Authentication & Access Control

- SIP services are secured with strong authentication policies and rate limiting to block brute-force attempts.
- All internal systems follow role-based access control (RBAC) and require multi-factor authentication (MFA).

3. Infrastructure Hardening

- Systems are routinely updated with the latest security patches.
- Voice servers and web portals are isolated within tightly controlled network segments.

4. Monitoring & Incident Response

- We provide 24/7 monitoring across all systems for anomaly detection and alerting.
- A tested incident response plan ensures swift containment and resolution of any security event.

5. Customer Data Protection

- Customer data is handled in compliance with GDPR, CCPA, and other applicable regulations.
- All backups are encrypted and regularly tested as part of our disaster recovery planning.

6. Regulatory Compliance

Headland Communications is committed to compliance with all relevant telecom security standards, including:

- FCC regulations
- STIR/SHAKEN for caller ID verification
- CALEA lawful intercept support, as required

7. Responsible Disclosure

We welcome reports from security researchers and customers. If you discover a vulnerability or have concerns, please contact our support team.

We take every report seriously and respond promptly.

Need More Info?

For additional information about our security posture or to request additional compliance documentation, contact our support team or your account manager.