

ROBOCALL MITIGATION PLAN

Advanced Network Communications LLC

Effective Date: August 29, 2026

Registered Address	1001 S. Main St. STE 600, Kalispell, MT 59901 USA
Chief Executive Officer	Md Jewel Rana
Robocall Mitigation Contact	Md Jewel Rana
Email	jewel@advancednetcom.lat
Telephone	406-253-4356
FCC Form 499 Filer ID	838733
D-U-N-S® Number	14-459-8785
State Entity ID	C1618227

Prepared as the Company's written robocall mitigation procedures and operational compliance framework.

Contents

1. Purpose and Commitment
2. Nature of Business and Services
3. Know Your Customer - KYC Program
4. Customer Business and Use-Case Verification
5. Enhanced Due Diligence for High-Volume Customers
6. Customer Risk Assessment
7. Customer Renewal and Ongoing KYC
8. Acceptable Use and Contractual Controls
9. Caller ID Controls
10. STIR/SHAKEN and Caller ID Authentication
11. Know Your Upstream Provider - KYUP
12. RMD Verification of Providers
13. Traffic Monitoring and Call Analytics
14. Third-Party Analytics
15. Complaint Monitoring
16. Traceback Response Policy
17. Traceback Escalation Procedure
18. Immediate Suspension for High-Risk Activity
19. Customer Enforcement
20. Repeat Violations
21. Telephone Number Management
22. Telemarketing and Consumer-Protection Compliance
23. Customer Certification
24. Downstream and Upstream Cooperation
25. FCC and Law-Enforcement Cooperation
26. Recordkeeping
27. Employee and Personnel Responsibility
28. Plan Review and Continuous Improvement
29. Material Changes
30. Robocall Mitigation Contact
31. Management Commitment
- Certification
- Appendix A - Important Filing Notes

1. PURPOSE AND COMMITMENT

Advanced Network Communications LLC ("ANC" or the "Company") maintains this Robocall Mitigation Plan to prevent its network, services, facilities, and telecommunications resources from being used to originate, carry, process, or facilitate illegal robocalls or other unlawful voice traffic.

ANC is committed to complying with applicable Federal Communications Commission ("FCC") robocall mitigation, caller identification authentication, traceback, Know Your Customer ("KYC"), Know Your Upstream Provider ("KYUP"), and call-blocking requirements.

ANC takes affirmative and effective measures intended to:

- Prevent customers from using ANC services to originate illegal calls.
- Identify suspicious or potentially unlawful calling activity.
- Prevent the transmission of high volumes of illegal traffic.
- Verify customers before providing voice services.
- Conduct additional due diligence for customers requesting high-volume calling services.
- Verify upstream telecommunications providers.
- Investigate complaints and traceback requests.
- Suspend or terminate customers involved in illegal calling activity.
- Block identified illegal traffic where appropriate.
- Cooperate with the FCC, law enforcement, the Industry Traceback Group ("ITG"), downstream carriers, upstream carriers, and other authorized entities investigating suspected illegal calls.

ANC does not knowingly permit its network or services to be used for fraudulent, deceptive, unlawful, spoofed, scam, impersonation, or otherwise illegal calling activity.

2. NATURE OF BUSINESS AND SERVICES

Advanced Network Communications LLC operates as a telecommunications and VoIP service provider.

ANC's services may include wholesale interconnected VoIP services, domestic U.S. voice termination, origination, SIP trunking, telephone-number services, and related telecommunications services.

Depending on the particular service and call flow, ANC may serve as an originating voice service provider, wholesale provider, or another provider within the voice call path.

ANC recognizes that high-volume voice services can present increased risk and therefore subjects customers requesting such services to enhanced verification, monitoring, and compliance procedures.

3. KNOW YOUR CUSTOMER - KYC PROGRAM

ANC maintains a Know Your Customer program designed to establish the identity and legitimacy of customers before activating voice services.

ANC does not rely solely on information supplied verbally by prospective customers.

Depending on the customer's business type, requested services, anticipated traffic volume, risk profile, and jurisdiction, ANC may obtain and review the following information:

Business Identification

- Full legal company name
- Trade or DBA names
- Business formation documents
- State registration information
- Registered business address
- Physical operating address
- Employer Identification Number ("EIN") or equivalent tax identification
- Website and business domain
- Business telephone numbers
- Corporate email addresses
- State Entity ID
- D-U-N-S® Number, where available

Telecommunications Regulatory Information

Where relevant to the services requested, ANC may verify:

- FCC Registration Number ("FRN")
- FCC Form 499 Filer ID
- Robocall Mitigation Database registration
- Operating Company Number ("OCN")
- Relevant state or federal telecommunications registrations
- STIR/SHAKEN implementation information
- Other applicable regulatory registrations

Responsible Persons

ANC may obtain information regarding:

- Owners
- Directors
- Officers
- Authorized representatives
- Compliance personnel
- Technical/NOC contacts
- Billing contacts

ANC may request identification or additional supporting documentation where necessary to confirm the identity of responsible individuals.

4. CUSTOMER BUSINESS AND USE-CASE VERIFICATION

Before activating voice services, ANC seeks to understand the customer's intended use of those services.

Customers may be required to disclose:

- Nature of the customer's business
- Intended calling purpose
- Types of campaigns
- Expected monthly call volume

- Expected daily call volume
- Expected CPS
- Expected concurrent channels
- Expected Average Call Duration ("ACD")
- Expected Answer-Seizure Ratio ("ASR")
- Geographic calling patterns
- Whether calls are inbound or outbound
- Whether automated dialing technology will be used
- Whether prerecorded or artificial-voice messages will be used
- Source and authorization for Caller ID numbers
- Whether the customer is acting as an end user, reseller, carrier, or service provider
- Identity of downstream end users where appropriate

ANC may request additional supporting documentation when a proposed use case presents elevated risk.

5. ENHANCED DUE DILIGENCE FOR HIGH-VOLUME CUSTOMERS

ANC recognizes the increased risk associated with high-volume voice origination.

Customers seeking significant CPS, channel capacity, bulk outbound calling capability, automated dialing, or similar high-volume services may be subject to enhanced review.

Enhanced due diligence may include:

- Additional corporate verification
- Confirmation of business operations
- Verification of physical address
- Verification of company officers
- Review of website and online presence
- Review of FCC registrations
- Review of RMD status
- Review of telecommunications history
- Review of customer references
- Verification of intended campaigns
- Verification of Caller ID ownership or authorization
- Additional compliance representations
- Review of complaint history
- Review of traceback history, where available

ANC reserves the right to decline service when a customer's identity, business purpose, source of traffic, or intended use cannot be satisfactorily verified.

6. CUSTOMER RISK ASSESSMENT

ANC evaluates customers based on the overall risk presented by their account and traffic.

Potential risk indicators include:

- Unverifiable corporate information
- Recently created entities with no identifiable business operations
- Inconsistent business information

- Unverified physical addresses
- Requests for unusually high call capacity without a legitimate explanation
- Repeated changes in originating IP addresses
- Frequent changes in Caller ID numbers
- High levels of short-duration calls
- Unusual traffic spikes
- Significant deviations from expected traffic profiles
- Excessive consumer complaints
- Traceback requests
- Fraud reports
- Brand-impersonation complaints
- Requests to use telephone numbers the customer cannot demonstrate authority to use
- Misrepresentation of calling purpose
- Attempts to conceal the true originator of traffic

Accounts displaying material risk indicators may be restricted, suspended, subjected to additional verification, or terminated.

7. CUSTOMER RENEWAL AND ONGOING KYC

ANC's customer-verification obligations do not end after initial activation.

ANC may periodically reverify customers and may conduct additional due diligence when:

- Services are renewed.
- Calling capacity is materially increased.
- Calling patterns materially change.
- New types of traffic are introduced.
- Account ownership changes.
- Corporate information changes.
- New IP addresses are introduced.
- New regulatory concerns arise.
- Complaints or traceback requests are received.
- ANC identifies other risk indicators.

Customers are expected to maintain accurate contact, ownership, regulatory, and business information.

8. ACCEPTABLE USE AND CONTRACTUAL CONTROLS

ANC prohibits customers from using its services to originate or facilitate illegal calls.

ANC's service terms, agreements, acceptable-use requirements, onboarding documents, or other contractual arrangements may prohibit activities including:

- Fraudulent calling
- Scam calls
- Government impersonation
- Financial-institution impersonation
- Retail-brand impersonation
- Technology-support scams
- Social-security scams

- Tax-related scams
- Healthcare scams
- Unauthorized telemarketing
- Calls violating applicable consumer-consent requirements
- Caller ID spoofing intended to defraud, cause harm, or wrongfully obtain anything of value
- Use of unauthorized telephone numbers
- Misleading Caller ID information
- Calls violating applicable federal or state laws
- Attempts to circumvent carrier fraud-prevention systems
- Attempts to conceal the true originating customer
- Reselling services without authorization when authorization is required

ANC reserves the contractual right to investigate, restrict, suspend, block, or permanently terminate services when illegal or suspicious activity is identified.

9. CALLER ID CONTROLS

ANC expects customers to use Caller ID information that they own or are authorized to use.

ANC may require customers to provide evidence demonstrating authorization to use particular telephone numbers.

ANC prohibits customers from intentionally transmitting false or misleading Caller ID information for fraudulent or unlawful purposes.

Where technically feasible and appropriate, ANC may employ controls designed to detect:

- Invalid Caller IDs
- Malformed Caller IDs
- Obviously spoofed numbers
- Unauthorized numbering patterns
- Excessive Caller ID rotation
- Caller IDs associated with complaints or fraud reports

Numbers confirmed to be associated with illegal traffic may be blocked or removed from service.

10. STIR/SHAKEN AND CALLER ID AUTHENTICATION

ANC supports the objectives of the STIR/SHAKEN caller ID authentication framework.

ANC will accurately report its applicable STIR/SHAKEN implementation status in its FCC Robocall Mitigation Database certification.

For traffic subject to STIR/SHAKEN requirements, ANC will implement or utilize caller ID authentication procedures consistent with applicable FCC requirements and the Company's role in the call path.

ANC will not intentionally assign an authentication level inconsistent with information reasonably available concerning the customer and the customer's authorization to use the calling number.

Where ANC relies on another provider or technology vendor for STIR/SHAKEN-related functionality, ANC will take reasonable measures to ensure that the applicable service is being appropriately utilized.

11. KNOW YOUR UPSTREAM PROVIDER - KYUP

ANC performs reasonable due diligence concerning telecommunications providers from which it directly receives voice traffic.

Depending on the relationship, ANC may obtain or verify:

- Legal company name
- Business address
- Physical business location
- Country and state of organization
- Tax identification information
- Responsible contact person
- NOC contact
- Compliance contact
- FCC Registration Number
- FCC Form 499 registration
- Robocall Mitigation Database status
- OCN, where applicable
- Nature of business
- Nature and expected volume of traffic
- STIR/SHAKEN status where applicable

ANC evaluates upstream providers for indications that they may be transmitting a high volume of illegal traffic.

ANC may restrict or terminate an upstream relationship when reasonable investigation establishes that the upstream provider is transmitting illegal traffic and fails to take effective corrective action.

12. RMD VERIFICATION OF PROVIDERS

Where applicable under FCC rules, ANC checks the Robocall Mitigation Database status of telecommunications providers with which it establishes direct voice interconnections.

ANC will not knowingly establish or continue a direct traffic relationship prohibited by FCC RMD requirements.

ANC may periodically recheck provider registrations because an RMD certification can be updated, removed, or otherwise changed.

13. TRAFFIC MONITORING AND CALL ANALYTICS

ANC utilizes network information, internal monitoring tools, carrier information, complaint data, and other available analytics to identify potentially suspicious traffic.

ANC's monitoring may consider indicators including:

- Call volume
- Calls per second
- Concurrent calls
- Answer-Seizure Ratio
- Average Call Duration
- Short Duration Percentage

- Unanswered-call ratios
- Repeated sequential dialing
- Traffic spikes
- Destination patterns
- Caller ID patterns
- Excessive Caller ID rotation
- Invalid or malformed Caller IDs
- Geographic inconsistencies
- Customer-specific baselines
- Complaint frequency
- Traceback frequency
- Fraud notifications
- Carrier blocking reports
- Abnormal changes in traffic behavior

No single metric automatically establishes that calls are illegal.

ANC considers relevant information collectively and investigates suspicious patterns before determining the appropriate mitigation response, except where immediate protective action is warranted.

14. THIRD-PARTY ANALYTICS

ANC may rely on analytics, fraud-detection information, reputation information, traceback information, blocking information, or other data provided by:

- Underlying carriers
- Interconnected carriers
- Terminating carriers
- Technology vendors
- Industry traceback organizations
- Numbering providers
- Fraud-prevention services
- Government agencies
- Law-enforcement authorities

ANC also utilizes its own network information and customer records when investigating suspicious traffic.

Any specific third-party analytics provider required to be disclosed in ANC's RMD certification will be accurately identified in the applicable filing.

15. COMPLAINT MONITORING

ANC takes complaints involving suspected illegal calls seriously.

Complaints may originate from:

- Consumers
- Upstream carriers
- Downstream carriers
- Terminating carriers

- Industry Traceback Group
- FCC
- Law enforcement
- Numbering providers
- Fraud-prevention organizations
- Brand owners
- Other telecommunications providers

ANC may correlate complaint information with:

- Call Detail Records ("CDRs")
- SIP signaling
- Account records
- Customer IP information
- Calling and called numbers
- Date and time
- Carrier routing information
- STIR/SHAKEN information
- Customer identity
- Campaign information

When evidence indicates customer involvement in unlawful activity, ANC may immediately restrict or suspend the account pending further investigation.

16. TRACEBACK RESPONSE POLICY

ANC commits to responding fully to traceback requests from:

- The Federal Communications Commission
- Law-enforcement authorities
- The Industry Traceback Consortium/Industry Traceback Group
- Other entities authorized under applicable FCC requirements

ANC's policy is to provide a complete response within 24 hours of receiving a valid traceback request.

ANC will make reasonable efforts to determine:

- Whether the call traversed ANC's network
- The ANC customer responsible for the call
- The immediate upstream provider, where applicable
- The immediate downstream provider, where applicable
- Relevant source IP information
- Call timestamps
- Calling number
- Called number
- Relevant CDR information

ANC will cooperate with authorized investigations into suspected illegal calling activity.

17. TRACEBACK ESCALATION PROCEDURE

Step 1 - Locate the Call

ANC searches available CDR and network records using the calling number, called number, timestamp, IP address, and other available information.

Step 2 - Identify the Source

ANC identifies the customer or immediate upstream provider responsible for delivering the traffic.

Step 3 - Preserve Relevant Information

Relevant account, network, and call information is preserved consistent with applicable requirements and ANC policies.

Step 4 - Assess the Risk

ANC reviews the source account and determines whether the incident appears isolated or part of a broader pattern.

Step 5 - Restrict Traffic When Necessary

ANC may temporarily block a number, trunk, IP address, customer account, or other network resource where appropriate.

Step 6 - Request Customer Explanation

ANC may require the customer to explain the call, identify the campaign, demonstrate authorization, and provide supporting evidence.

Step 7 - Respond to the Traceback

ANC provides responsive information to the requesting authorized entity within the applicable deadline.

Step 8 - Corrective Action

Depending on investigation results, ANC may warn, restrict, suspend, or permanently terminate the responsible customer.

18. IMMEDIATE SUSPENSION FOR HIGH-RISK ACTIVITY

ANC may immediately suspend traffic without advance notice when ANC identifies credible evidence involving:

- Government impersonation
- Amazon or other retail-brand impersonation
- Bank or financial institution impersonation
- Fraudulent technical-support calls
- Calls seeking passwords, PINs, CVVs, or one-time passwords
- Fraudulent payment requests
- Threatening government or law-enforcement impersonation
- Caller ID spoofing associated with fraud
- Repeated illegal robocall complaints
- Material misrepresentation during customer onboarding
- Failure to cooperate with a compliance investigation
- Attempts to circumvent previous blocks

Suspension may remain in effect until ANC determines that continued service does not present an unreasonable compliance risk.

19. CUSTOMER ENFORCEMENT

ANC applies mitigation measures proportionate to the nature and seriousness of identified activity.

Potential actions include:

1. Compliance warning
2. Request for supporting documentation
3. Additional KYC review
4. Traffic restriction
5. CPS reduction
6. Channel reduction
7. Blocking specific Caller IDs
8. Blocking destination patterns
9. Blocking source IP addresses
10. Temporary trunk suspension
11. Account suspension
12. Removal of telephone numbers
13. Permanent service termination
14. Notification to appropriate upstream or downstream providers
15. Cooperation with regulatory or law-enforcement authorities

ANC may proceed directly to permanent termination when the evidence establishes serious fraudulent or illegal conduct.

20. REPEAT VIOLATIONS

ANC does not permit customers to repeatedly use its services for illegal calling activity.

Customers responsible for repeated credible complaints, fraud events, or illegal call activity may be permanently terminated.

A customer terminated for serious illegal activity may be prohibited from opening another account under:

- A different company name
- An affiliate
- A related individual
- Another email address
- Another IP address
- Another payment method

where ANC reasonably determines that the new account is attempting to circumvent enforcement.

21. TELEPHONE NUMBER MANAGEMENT

ANC may take measures regarding telephone numbers associated with illegal activity.

Depending on the circumstances, ANC may:

- Remove a DID from a customer account
- Block the number from origination
- Disable routing
- Investigate ownership

- Notify the numbering provider
- Prevent reassignment to the same offending customer
- Preserve relevant assignment records

ANC will cooperate with numbering providers and authorized investigators when telephone numbers are implicated in illegal traffic.

22. TELEMARKETING AND CONSUMER-PROTECTION COMPLIANCE

ANC requires customers to comply with applicable federal and state calling laws and regulations.

Customers are responsible for determining whether their calling campaigns require:

- Prior express consent
- Prior express written consent
- Do-Not-Call screening
- Internal Do-Not-Call procedures
- Calling-hour restrictions
- Artificial or prerecorded voice disclosures
- Identification requirements
- Opt-out mechanisms
- State-specific registrations or requirements

ANC does not represent to a customer that use of ANC's network eliminates the customer's independent legal obligations.

23. CUSTOMER CERTIFICATION

ANC may require customers to certify that:

- Their traffic is lawful.
- Their business information is accurate.
- They are authorized to use submitted Caller IDs.
- They will comply with applicable telecommunications laws.
- They will cooperate with traceback investigations.
- They will promptly investigate complaints forwarded by ANC.
- They will provide end-user information where lawfully required.
- They will not knowingly transmit illegal calls.
- They will not attempt to evade ANC's fraud or robocall-mitigation controls.

Providing false information may constitute grounds for immediate account termination.

24. DOWNSTREAM AND UPSTREAM COOPERATION

ANC cooperates with interconnected telecommunications providers to investigate and stop illegal calls.

ANC may exchange appropriate call-path information with carriers when necessary to:

- Complete tracebacks
- Identify illegal traffic
- Determine the originating source
- Block illegal traffic
- Prevent future recurrence

- Protect consumers
- Meet regulatory obligations

ANC will cooperate with providers on both sides of the call path consistent with applicable law and privacy requirements.

25. FCC AND LAW-ENFORCEMENT COOPERATION

ANC will cooperate with lawful requests from:

- Federal Communications Commission
- Federal Trade Commission
- State Attorneys General
- Federal law-enforcement agencies
- State or local law-enforcement agencies
- Industry Traceback Group
- Other legally authorized entities

ANC will preserve and provide records when required by applicable law or valid legal process.

26. RECORDKEEPING

ANC maintains records appropriate to operating and monitoring its telecommunications services.

Such records may include:

- Customer KYC documents
- Corporate registration documents
- Regulatory registration information
- Customer contracts
- Accepted terms
- Caller ID authorizations
- IP addresses
- Call Detail Records
- Traffic statistics
- Complaints
- Traceback requests and responses
- Suspension records
- Termination records
- Compliance correspondence
- Investigation notes

Records are maintained and protected consistent with applicable legal, regulatory, security, privacy, and operational requirements.

27. EMPLOYEE AND PERSONNEL RESPONSIBILITY

Personnel involved with customer onboarding, network operations, fraud prevention, carrier relations, or compliance are expected to escalate suspicious activity to appropriate management.

Relevant personnel are instructed not to ignore:

- Traceback requests
- Repeated customer complaints

- Fraud warnings
- Carrier notifications
- Suspicious traffic anomalies
- Evidence of caller ID abuse
- Requests from customers attempting to evade compliance controls

Management may update procedures as new illegal calling methods and risk patterns emerge.

28. PLAN REVIEW AND CONTINUOUS IMPROVEMENT

ANC periodically reviews this Robocall Mitigation Plan and its operational procedures.

The Company may strengthen or modify its mitigation measures based on:

- New FCC requirements
- FCC enforcement actions
- Changes in calling patterns
- Industry fraud trends
- Customer behavior
- Traceback experience
- Carrier feedback
- Changes in network technology
- Changes in STIR/SHAKEN requirements
- New analytics capabilities

ANC intends for its robocall mitigation program to evolve as threats and regulatory requirements change.

29. MATERIAL CHANGES

ANC will maintain accurate information in its FCC Robocall Mitigation Database filing.

Material changes to information submitted to the FCC will be reviewed by the Company's responsible personnel and the applicable filing will be updated as required.

Examples may include changes involving:

- Legal company name
- Business address
- Robocall mitigation contact
- Company ownership or principals
- STIR/SHAKEN implementation
- Provider role
- Affiliates or subsidiaries
- Material changes to this mitigation program
- Other information required by the FCC

30. ROBOCALL MITIGATION CONTACT

Questions, traceback matters, fraud complaints, regulatory inquiries, and robocall mitigation concerns involving Advanced Network Communications LLC should be directed to:

Name	Md Jewel Rana
-------------	---------------

Title	Chief Executive Officer
Company	Advanced Network Communications LLC
Address	1001 S. Main St. STE 600, Kalispell, MT 59901 USA
Telephone	406-253-4356
Email	jewel@advancednetcom.lat

ANC intends to maintain this contact information so authorized parties can promptly reach the Company regarding suspected illegal traffic.

31. MANAGEMENT COMMITMENT

Advanced Network Communications LLC recognizes its responsibility to protect U.S. consumers and the telecommunications ecosystem from illegal calls.

ANC is committed to:

- Knowing its customers.
- Knowing its immediate upstream providers.
- Conducting enhanced due diligence for higher-risk customers.
- Monitoring its network for suspicious activity.
- Investigating complaints.
- Responding fully to valid traceback requests within 24 hours.
- Cooperating with carriers and authorized authorities.
- Suspending or terminating entities responsible for illegal traffic.
- Continuously improving its robocall mitigation program.

ANC will not knowingly permit its telecommunications services to be used as a platform for unlawful robocalling, fraud, impersonation, or other illegal calling activity.

CERTIFICATION

I, Md Jewel Rana, Chief Executive Officer of Advanced Network Communications LLC, certify that I have reviewed this Robocall Mitigation Plan and that Advanced Network Communications LLC intends to implement and comply with the procedures and controls described herein.

I understand that the Company's Robocall Mitigation Database certification and mitigation plan must accurately reflect the Company's actual practices and operations.

Company	Advanced Network Communications LLC
Name	Md Jewel Rana
Title	Chief Executive Officer
Signature	_____
Date	_____

APPENDIX A - IMPORTANT FILING NOTES

This appendix is included because the complete matter accompanying the plan also addressed practical FCC filing considerations.

Operational accuracy. The Company should actually follow every material practice described in this plan. A written plan should reflect real operational procedures rather than generic statements or commitments that are not implemented in practice.

Specific measures. The plan is intentionally structured around concrete KYC, high-volume-customer vetting, Know Your Upstream Provider procedures, analytics, complaint handling, traceback response, suspension, blocking, and termination measures.

STIR/SHAKEN status. The exact STIR/SHAKEN implementation status is intentionally stated neutrally in this document. Before filing, Advanced Network Communications LLC should ensure that its Robocall Mitigation Database certification accurately identifies whether its implementation is Fully Implemented, Partially Implemented, or Not Implemented, as applicable to the Company's actual network and regulatory status.

Traceback response. The plan states a policy of providing a complete response within 24 hours of receiving a valid traceback request. Internal procedures and staffing should support that commitment.

Review before submission. Before submission to the FCC, the Company should review the plan against its actual current network architecture, customer onboarding workflow, STIR/SHAKEN implementation, analytics tools, third-party vendors, record-retention practices, and responsible compliance contacts, and revise any statement that is not accurate.

Reference Materials Mentioned in the Accompanying Filing Guidance

- Federal Communications Commission - FCC robocall mitigation and Robocall Mitigation Database orders, rules, public notices, and enforcement materials.
- FCC materials addressing deficiencies in robocall mitigation plans and the need for concrete, effective mitigation practices.
- FCC materials concerning identity verification, heightened scrutiny for high-volume voice customers, traceback cooperation, and provider due diligence.

Note: This document is a compliance-plan draft and is not legal advice. The Company should confirm the final filing against current FCC requirements and its actual operating practices before certification or submission.