> 需泰国律师审阅后正式启用 / Admin-only: requires review by a Thai lawyer before official activation

Nexora AI Call Acceptable Use and Anti-Fraud Policy

Version 1.1.0 · Effective date: 1 December 2026

Issued by [บริษัท สยามวอยซ์ เอไอ จำกัด / Siam Voice AI Co., Ltd.] ("**Nexora AI Call**"), Tax ID [เลขประจำตัวผู้เสียภาษี 13 หลัก], [ที่อยู่สำนักงานใหญ่ / Head office address], Bangkok.

1. Purpose and scope

1.1 Nexora AI Call lets users place and receive AI-assisted calls, translation bridge calls, SMS and LINE messages. Telephone fraud causes serious harm to people in Thailand and abroad. This Acceptable Use Policy ("**AUP**") sets the rules for everyone who uses the Service, to protect call recipients, telecom networks and the public.
1.2 The AUP applies to consumers, business Customers, their Authorised Users, API users, resellers and agents, and any person using a Nexora AI Call number, API Key or account ("**User**"). It is incorporated into the Terms of Service for Consumers, the Terms of Service for Business and every reseller and enterprise agreement. Users are responsible for the acts of those they allow to use their account or API Keys.
1.3 In case of conflict, the stricter rule applies. Nothing in this AUP limits Nexora AI Call's right to act where required by law.

2. Core principles

2.1 **Transparency.** The AI always discloses at the start of a call that it is an AI assistant and, for a business call, names the business on whose behalf it calls. This cannot be disabled. Users must not instruct, script or configure the AI to deny being an AI, to pretend to be a named human, or to impersonate any real person.
2.2 **Lawfulness and consent.** Users may only contact people they have a lawful basis to contact, in accordance with the Personal Data Protection Act B.E. 2562 (2019), the Telecommunications Business Act B.E. 2544 (2001), the Computer Crime Act B.E. 2550 (2007), the Consumer Protection Act and other applicable law.
2.3 **Verified identity.** Users must be truthfully identified to Nexora AI Call through KYC (levels L0 to L3). Limits on spend, daily calls and new numbers depend on level.

3. Prohibited: fraud and scam calls and messages

Users must not use the Service, directly or through the AI, to carry out, support or prepare any scam, deception or unlawful inducement, including:

3.1 **Impersonation of authorities and institutions.** Pretending to be, or to act for, the police, a prosecutor, a court, the Department of Special Investigation, the Anti-Money Laundering Office, the Revenue

Department, customs, immigration, a government agency, a bank or financial institution, a payment or e-wallet provider, a telecom operator, a courier, a utility or an embassy, or using their names, titles, logos or scripts to alarm or mislead recipients.
3.2 **"Safe account" and transfer scams.** Telling or inducing a person to transfer money to a "safe", "verification", "government" or "escrow" account, to hand over funds, to purchase vouchers or crypto-assets, to install remote-access software or banking apps at the caller's direction, or to disclose OTPs, PINs, passwords, card numbers or ID data.
3.3 **Parcel and customs scams.** False claims that a parcel contains illegal goods, that duties or fines are owed, or that the recipient is under investigation, in order to extract money or data.
3.4 **Investment, job, loan and romance scams.** Guaranteed or abnormally high returns, pyramid or Ponzi schemes, unlicensed securities or crypto-asset or forex offers, fake job or task-for-pay offers, advance-fee loans, fake charity or disaster appeals, and building false romantic or personal relationships to obtain money.
3.5 **Phishing and credential harvesting**, including sending links to fake sites by SMS or LINE and soliciting login details.
3.6 **Impersonating relatives or employers** ("hello, it's me"), and "SIM-box", call-masking or call-forwarding arrangements intended to hide the true origin of traffic.
3.7 **Mule-account and money-laundering activity**, including recruiting or paying people to open or lend bank, e-wallet or SIM accounts.
3.8 Any other act intended to deceive a person into harming their own property, rights or safety.

The Service uses keyword, pattern and model-based detection (for example, phrases such as "โอนเงิน", "police", "parcel customs", "安全账户" in suspicious contexts) and fraud scoring to allow, review or block traffic.

4. Caller ID and number rules

4.1 Every caller ID or sender ID must be a number that the User owns, lawfully rents, rents from Nexora AI Call or has proven control of by OTP verification (call or SMS). Enterprise numbers must be bound to the business registration (tax ID/DBD number).
4.2 **Spoofing is prohibited**: displaying a number or sender name the User has no right to use, altering or masking caller ID to mislead, using numbers of government bodies, banks or other persons, or using international traffic made to look local.
4.3 Numbers that cannot be verified are rejected. Numbers may be suspended or recalled where used in breach of this AUP.
4.4 Users must not obtain numbers or SIMs using false identities and must not transfer numbers to third parties without Nexora AI Call's approval.
4.5 **Verification and records.** Caller IDs and sender IDs are verified by an OTP call or SMS sent to the number, and a verified number is re-verified when ownership may have changed or on Nexora AI Call's request. Enterprise numbers and sender IDs are registered against the business's registration record and, where required, registered with the telecom operator.
4.6 Sender-ID registrations, number allocation records (which number was assigned to which end customer, and when) and the related end-customer KYC records are kept and may be disclosed to telecom operators

and to the National Broadcasting and Telecommunications Commission (NBTC) for carrier audits, complaint handling and regulatory compliance. Users agree to supply accurate information for these records and to keep it up to date.
4.7 A number may be suspended at once, without prior notice, if ownership cannot be shown, if it is reported for spoofing or fraud, or if a carrier or authority so requires.

5. Prohibited content

Users must not send, play or generate through the Service content that:
5.1 is unlawful, defamatory, obscene, or exploits or sexualises minors;
5.2 threatens, intimidates, blackmails or incites violence or hatred, including on grounds of race, nationality, religion or gender;
5.3 infringes intellectual property, privacy or confidentiality, or discloses another person's personal data without lawful basis;
5.4 contains malware, malicious links or attempts to defeat security;
5.5 offers or promotes illegal drugs, weapons, human trafficking, counterfeit goods, unlicensed medicines or health products, or any other unlawful goods or services;
5.6 violates the lese-majeste law or other Thai laws on content that Thai authorities require to be removed, or false information likely to damage public order or national security under the Computer Crime Act;
5.7 uses synthetic or cloned voices of a real person without that person's clear consent, or deceptively imitates a real person.

6. Illegal gambling and restricted activities

6.1 Promotion, recruitment, payment collection or customer service for online or offline gambling, lotteries, betting or casino services that are not lawfully licensed in Thailand is prohibited, as are links, referral codes and promotions for them.
6.2 Unlicensed financial services, deposit-taking, money transfer or crypto-asset exchange, unlicensed debt collection that uses threats or disclosure of debts to third parties, and pyramid or multi-level schemes that breach the law are prohibited.
6.3 Regulated activities (for example, insurance, securities, healthcare, alcohol and tobacco promotion) may be conducted only by a licensed party in compliance with the applicable advertising rules, and Nexora AI Call may require evidence of licences.

7. Harassment and abuse

7.1 Users must not use the Service to harass, stalk, threaten, or repeatedly contact a person who has asked not to be contacted, or to make "prank", silent or abusive calls.
7.2 Repeated calls or messages to the same person beyond reasonable frequency, "wangiri" (one-ring) calls, traffic pumping, and autodial patterns intended to annoy are prohibited.
7.3 Debt collection by the Service must follow applicable Thai debt-collection rules: no threats, no contact with third parties about the debt, no contact at unreasonable hours and no false claims of legal action.

8. Political, election and public-opinion calls

8.1 Robocalls and automated messages for political campaigning, election, referendum or lobbying purposes may be sent only by or for lawfully registered parties, candidates or organisations, in compliance with the Election Commission's rules, with clear identification of the sponsor, with required consent, and never during any legally restricted election-silence period.
8.2 Disinformation, fake polls, impersonation of candidates, officials or electoral bodies, and voice-cloned messages in the name of public figures are prohibited. Nexora AI Call may block such campaigns pending verification.

9. Protection of children

9.1 Users must not knowingly direct calls or marketing at children under 15, or collect personal data from them without a parent's or guardian's consent.
9.2 Content that is harmful to minors, grooming, or sexual content involving minors is strictly prohibited and will be reported to the authorities immediately.
9.3 Products unsuitable for minors (for example, alcohol, gambling, adult content) must not be promoted to persons who may be minors.

10. Spam, marketing and consent

10.1 Bulk, unsolicited or deceptive commercial communications are prohibited. Marketing SMS, LINE and calls require prior consent where the law requires it, and the User must keep and, on request, show proof of consent.
10.2 Every marketing SMS must include an opt-out instruction. Opt-out keywords STOP, ยกเลิก, 退订, หยุด and UNSUBSCRIBE are processed immediately and in any case within twenty-four (24) hours across all systems; one confirmation SMS is sent. Users must not message opted-out numbers.
10.3 Users must not buy, rent or scrape contact lists without lawful basis, use harvested data, send to randomly generated numbers, or conceal the sender's identity or the commercial nature of the message.
10.4 Message content must not use misleading subject lines, false urgency, or links that disguise their destination.

11. Calling hours

11.1 Default permitted calling hours are 08:00 to 20:00 Asia/Bangkok. Marketing calls and messages are permitted only 09:00 to 18:00 on weekdays (not public holidays unless the recipient has agreed).
11.2 Users must not circumvent hour controls by changing time zones or schedule settings. Urgent service notifications outside these hours are allowed only where the recipient expects them and they are not marketing.
11.3 Recipients' time zone is respected for calls to recipients abroad (the hours of the recipient's local time apply where stricter).

12. Do-not-call and blacklists

12.1 Users must not contact numbers registered on do-not-call lists maintained by law or by Nexora AI Call, numbers that have opted out, or numbers on the User's own suppression list.
12.2 Nexora AI Call screens campaigns against the platform blacklist and opt-out registry. Attempts to bypass screening (for example, by altering digits or splitting lists) are a serious breach.
12.3 If a recipient says "do not call me again" to the AI, the AI records the request and the number is added to suppression immediately.

13. Security and system integrity

Users must not probe, scan or test the vulnerability of the Service without written permission; overload or disrupt it; evade rate limits, fraud controls or billing; share or sell API Keys; use the Service to attack others; or access another Tenant's data.

13A. Toll-fraud prevention and traffic controls

13A.1 **Thai destinations only by default.** Outbound calls and SMS are by default permitted only to Thai numbers (+66 mobile and fixed-line). All other destinations are blocked.
13A.2 **International and premium destinations on request only.** International destinations, premium-rate and special numbers (for example 1900 numbers, other service numbers beginning with 1, and satellite numbers) are blocked unless a Nexora AI Call platform administrator enables them for the User's tenant after a written request. Enabling may require a higher KYC level, a written business justification, a deposit or prepayment [amount, configurable], lower caps, internal approval, and may be limited to named countries or prefixes. It may be withdrawn at any time. Users must not try to reach blocked destinations by other routes, forwarding, call-back or bridging.
13A.3 **Caps.** Each account is subject to caps on concurrent calls, daily call minutes and daily spend in THB, which depend on KYC level and plan. The defaults are configuration settings set by Nexora AI Call and may change; a User may ask for an increase, which is reviewed against risk and KYC level. Per-call limits on duration and AI usage cost also apply.
13A.4 **Night-time anomaly cut-off.** An unusual burst of traffic between 22:00 and 07:00 Asia/Bangkok automatically opens a circuit breaker and stops outbound traffic from the affected account, number or key until it is reviewed by Nexora AI Call. Users who need legitimate night-time campaigns must request this beforehand and still comply with the calling hours in Section 11.
13A.5 **No revenue-sharing and pumping schemes.** Users must not generate calls or messages to numbers in which they or their associates have a revenue-sharing, termination or other financial interest (International Revenue Share Fraud, traffic pumping), nor use wangiri patterns.
13A.6 **Credential security and responsibility.** Users must protect passwords, 2FA devices and API Keys and must notify Nexora AI Call immediately of suspected compromise. As between the User and Nexora AI Call, the User is responsible for traffic generated through its credentials until it has notified Nexora AI Call and Nexora AI Call has had reasonable time to act, to the extent provided by the Terms or agreement. Nexora AI Call may hold wallet credit to cover fraudulent charges.

13A.7 **Trial and promotion abuse.** The free trial is limited to one per verified phone number, device fingerprint and IP address (subject to rate limits); disposable e-mail addresses are blocked; and trial calls are limited to the User's own verified or approved numbers. Opening multiple accounts to obtain more trials, credits or coupons, using one coupon repeatedly beyond its limits, self-referral, circular referrals, or manufacturing referrals to earn commission is prohibited. Nexora AI Call may revoke the coupon, credit or commission, claw back related amounts, and suspend or close the accounts concerned.
13A.8 **Misuse of AI and prompt injection.** Users must not configure prompts, scripts, knowledge-base content or tools so that the AI deceives, pressures or extracts secrets from call recipients; must not attempt to obtain another Tenant's data, system prompts, credentials or hidden instructions from the AI; must not deliberately feed content designed to hijack the AI (prompt injection) or to disable its safeguards; and must not use the AI to produce scam scripts. The AI treats caller speech and uploaded content as untrusted data, uses an allow-list of tools, filters its output and blocks listed sensitive or scam keywords in speech and SMS; the AI hands over to a human or ends the call where it cannot proceed safely.

14. Monitoring and review

14.1 Nexora AI Call monitors risk signals: new accounts, KYC level, bursts of traffic, many distinct numbers, high ratios of very short calls, complaints and flagged content. A fraud risk score determines whether activity is allowed, queued for review or blocked.
14.2 Nexora AI Call randomly samples outbound call and SMS transcripts, and reviews flagged content, to detect abuse. Reviews are limited to authorised staff, are logged in a tamper-evident audit log, and are performed under the Privacy Policy and the Terms.
14.3 Users must keep records enabling them to show lawful basis, consent and the identity of the business on whose behalf messages are sent, and cooperate with reasonable verification requests.

14.4 **Content sampling and review disclosure.** Nexora AI Call samples a random percentage of outbound call and SMS transcripts and also queues content flagged by keyword or language-model scam detection (for example "โอนเงิน", "police", "parcel customs", "安全账户") for review by authorised Nexora AI Call operations staff. By using the Service Users acknowledge this review, and Business Customers must ensure that their own privacy notices and recording notices do not conflict with it. Reviewed content may lead to enforcement under Section 15, and may be disclosed to telecom operators and authorities as described in Section 16.
14.5 **Fraud scoring.** A fraud risk score is calculated per account and per call from signals such as account age, KYC level, bursts, number of distinct destinations, short-call ratio, complaints, flagged content, destination and spend patterns, and trial-abuse signals, and results in allow, review or block. A User who is blocked may ask for human review (Section 17).
14.6 **Login and device security.** Nexora AI Call analyses IP address (geolocation and network), browser/device fingerprint and login history to detect account takeover, sends alerts for logins from a new device or unusual location, and may require re-verification. Two-factor authentication is mandatory for Nexora AI Call staff and enterprise owners and finance users.
14.7 **Reports to carriers and NBTC.** Fraud reports, complaints and suspensions may be reported to telecom operators and to the NBTC periodically and per incident, as required by carrier agreements and law.

15. Enforcement ladder

Nexora AI Call applies measures proportionate to the severity, history and risk, and may skip steps where fraud, danger to people or legal order requires:

1. **Warning**: written notice identifying the concern and a deadline to correct.
2. **Throttling**: reduction of daily spend, call volume or new-number limits, or additional review of campaigns, for example moving to manual approval.
3. **Suspension**: one-click suspension of a number, API Key, campaign or the whole Tenant's outbound traffic, with an incident opened; lifting a number suspension requires approval by a second authorised staff member. Wallet credit may be held pending investigation.
4. **Termination**: closing the account and releasing numbers, with refund only as permitted by the Terms and not to the extent that credit is needed to meet losses, fines or third-party claims, or is seized under lawful order.
5. **Reporting to authorities**: where unlawful conduct is suspected, Nexora AI Call may report to and cooperate with the Royal Thai Police, the Technology Crime Suppression Division (TCSD), the National Broadcasting and Telecommunications Commission (NBTC), the Anti-Money Laundering Office, the Bank of Thailand or banks and payment providers, the Personal Data Protection Committee Office, the Consumer Protection Board and other competent authorities, in Thailand or abroad where lawful.

Immediate suspension without prior warning applies to scam activity, impersonating authorities, spoofing, child exploitation, imminent harm, or a lawful order. Nexora AI Call will tell the User the reason afterwards unless prohibited by law or likely to prejudice an investigation. Suspension and termination do not relieve the User of liability for fees or for loss caused.

16. Cooperation with law enforcement

16.1 Nexora AI Call responds to lawful requests, court orders and warrants from competent Thai authorities and, where lawful and appropriate, foreign authorities through proper channels. We verify the authority and scope of each request.
16.2 In response we may preserve and disclose account information, KYC documents, call detail records, recordings, transcripts and logs, to the extent required or permitted by law, including PDPA exemptions for compliance with law and for the protection of life, body and health. Where a telecom operator or the NBTC requires it for audit or complaint handling, we may also disclose end-customer KYC, sender-ID and number allocation records and fraud-report data to them, under confidentiality obligations.
16.3 We may preserve data for longer than normal retention periods where required for a legal hold or an investigation. Users should not expect notice of a request where the law or authority prohibits it.
16.4 Users must cooperate with Nexora AI Call's investigations and requests for information within five (5) business days (shorter in urgent cases).

17. Appeals

17.1 A User who believes an action was wrongly taken may appeal within fourteen (14) days by writing to [support@example.co.th] with the ticket number, the explanation and supporting evidence (for example, proof of consent, business registration, licences or number ownership).
17.2 A reviewer who was not involved in the original decision will respond within seven (7) business days, or give a reasoned update if more time is needed. Possible outcomes: reinstatement, reinstatement with conditions, or confirmation of the action.
17.3 Appeals do not suspend an action necessary to prevent immediate harm. Where authorities have asked Nexora AI Call to act, Nexora AI Call may be unable to reverse the action. Rights under law, including to complain to a regulator or to bring proceedings, are unaffected.

18. Reporting fraud and abuse

18.1 If you receive a suspicious call or message that appears to come from a Nexora AI Call number, or you see abuse of the Service, report it to [support@example.co.th] (subject "Fraud report") or [เบอร์โทรศัพท์], with the number, date and time, a description and any screenshots or recordings.
18.2 Fraud reports are triaged at the highest priority (P1) and reviewed within one (1) hour during support hours; confirmed cases lead to immediate suspension.
18.3 Victims should also report to the Thai police (including the online report channel of the Technology Crime Suppression Division), call their bank immediately to freeze transfers, and may contact the 1441 hotline of the Anti-Online-Scam Operation Center where appropriate. Nexora AI Call will support victims and authorities with relevant information to the extent permitted by law.
18.4 Nexora AI Call does not retaliate against good-faith reporters.

19. Responsibility of Customers and resellers

19.1 Business Customers must provide their personnel with training and internal policies consistent with this AUP, implement approval and monitoring for their campaigns, and promptly notify Nexora AI Call of any compromise or misuse.
19.2 Resellers and agents are responsible for the KYC of their sub-customers, must flow down this AUP, and are liable for sub-customer breaches as provided in their agreements. They must keep accurate number-allocation and sub-customer KYC records and make them available for carrier audits.

20. Changes

Nexora AI Call may update this AUP to reflect law, regulator guidance or new threats. Material changes are notified at least thirty (30) days in advance by e-mail or in-app notice, except that changes needed to prevent fraud or comply with law may take effect immediately. Continued use means acceptance.

21. Governing law and language

21.1 This AUP is governed by the laws of Thailand. Disputes are resolved as stated in the applicable Terms of Service or agreement.
21.2 This AUP exists in Thai, Chinese and English. **The Thai version governs in case of discrepancy.**

22. Contact

Support and fraud reports: [support@example.co.th] · Legal: [legal@example.co.th] · Data protection: [dpo@example.co.th] · Phone: [เบอร์โทรศัพท์] · Address: [ที่อยู่สำนักงานใหญ่ / Head office address], Bangkok.
