

NEURALBYTES CUSTOMER-CONTROLLED WORKFLOW AGREEMENT

Customer, partner, bridge access, API access, and AI-assisted automation

Page 1 of 6

LEGAL REVIEW RECOMMENDED

This professional template is not legal advice. Have a qualified attorney review before final use.

PART A Agreement Type

- | | | |
|---|---|---|
| <input type="checkbox"/> New customer workflow access | <input type="checkbox"/> Monthly bridge access | <input type="checkbox"/> Business / office workflow |
| <input type="checkbox"/> Partner / referral | <input type="checkbox"/> AI automation / API access | <input type="checkbox"/> One-time bridge session |

EFFECTIVE DATE

AGREEMENT TERM

INTERNAL REFERENCE ID

PART B Customer or Partner Information

LEGAL NAME / COMPANY NAME

DBA / TRADE NAME

AUTHORIZED CONTACT

TITLE / ROLE

EMAIL

PHONE

BILLING ADDRESS

SERVICE ADDRESS / COVERED LOCATION

- Customer owns or is authorized to manage covered systems.
- Customer is signing for a business or organization.
- Partner is requesting support for an authorized end customer.

NEURALBYTES CUSTOMER-CONTROLLED WORKFLOW AGREEMENT

Covered systems, access terms, and customer-authorized scope

Page 2 of 6

PART C Covered Systems and Plan Details

COVERED DEVICES

COVERED USERS

MONTHLY FEE / HOURLY RATE

COVERED DEVICES, SYSTEMS, ACCOUNTS, USERS, AND LOCATIONS

CUSTOMER-AUTHORIZED WORKFLOW SCOPE

EXCLUDED OR OUT-OF-SCOPE WORK

PART D Bridge Access Rules

Bridge access covers only the devices, users, locations, response expectations, API use, and workflows approved in writing. Customer chooses which workflows to request and authorize. Unused time does not roll over unless the written plan says otherwise. Emergency, after-hours, onsite, hardware, software licensing, third-party vendor, data recovery, regulated-data, or out-of-scope work may require separate written approval and additional fees.

SPECIAL ACCESS TERMS, API LIMITS, OR RESPONSE EXPECTATIONS

NEURALBYTES CUSTOMER-CONTROLLED WORKFLOW AGREEMENT

Customer control, remote agent access, AI automation, monitoring, and privacy

Page 3 of 6

PART E Customer-Directed Access Authorization

Customer authorizes use of the NeuralBytes bridge, relay, launcher, agent, and API only for customer-approved workflows on systems Customer owns, administers, or has permission to manage. Customer chooses the devices, requests, commands, timing, and whether access continues. Customer may end a session or request credential revocation at any time.

Customer authorizes bridge/agent/API access only for customer-approved workflow scope.

PART F AI-Assisted Automation

Customer understands NeuralBytes may provide AI-assisted tools, scripts, agents, recommendations, and automation as part of the bridge. Customer remains responsible for choosing and approving requested workflows. AI-assisted systems may make mistakes, misunderstand instructions, fail to resolve an issue, or produce incorrect recommendations.

Customer accepts customer-authorized AI-assisted automation and understands it may make mistakes.

PART G Monitoring, Audit Logs, and Replay

Customer consents to monitored sessions and records, including timestamps, session identifiers, API events, customer instructions, notes, command history, diagnostic output, screenshots, screen recordings, and replay timelines for security, quality control, customer review, troubleshooting, billing, and dispute resolution.

Customer consents to monitoring, audit logs, and replay records for approved workflows.

PART H Security, Sanitization, and Privacy

Customer controls what information is submitted through the bridge or API. Public traffic uses HTTPS/TLS. Server-side relay credentials are stored as hashes, but NeuralBytes does not claim full database or disk encryption at rest unless separately agreed. Customer should not provide passwords, payment data, private documents, health information, tax records, regulated data, or unnecessary sensitive information unless specifically required and handled through an appropriate secure method.

For internal datasets, training, tool improvement, routing, and documentation, NeuralBytes may use sanitized or de-identified workflow patterns. Long-term knowledge records should exclude raw customer records, screenshots, private documents, raw command transcripts, names, contact information, passwords, tokens, payment data, IPs, hostnames, full paths containing usernames, and unique identifiers where practical.

SPECIAL PRIVACY RESTRICTIONS OR HANDLING NOTES

NEURALBYTES CUSTOMER-CONTROLLED WORKFLOW AGREEMENT

Customer responsibility, backups, no guarantee, and limitation terms

Page 4 of 6

PART I Backup Responsibility

Customer is responsible for backing up important files, business records, QuickBooks data, email, photos, documents, passwords, recovery keys, licenses, databases, virtual machines, and other data before requesting or authorizing workflows. Customer should not run bridge, API, repair, automation, or agent work on critical systems without a current backup or a written decision to proceed without one.

- | | |
|--|---|
| <input type="checkbox"/> Important files/documents backed up | <input type="checkbox"/> Business/QuickBooks records backed up |
| <input type="checkbox"/> Passwords/recovery keys preserved | <input type="checkbox"/> Customer chooses to proceed without current backup |

Customer accepts backup responsibility before bridge, API, repair, or automation work.

PART J No Guaranteed Outcome

NeuralBytes may provide tools, relay access, automation, recommendations, and optional supervision, but does not guarantee any specific result, uptime, speed improvement, malware removal, data recovery, account recovery, system repair, business result, compatibility, or third-party service restoration.

Customer understands no specific workflow, repair, recovery, or business result is guaranteed.

PART K Limitation of Liability and Waiver

To the maximum extent permitted by law, NeuralBytes, its owners, operators, contractors, and representatives are not responsible for indirect, incidental, special, consequential, punitive, or business-interruption damages, including lost data, lost revenue, lost profits, downtime, corrupted files, failed updates, security incidents, third-party service failures, missing backups, or losses caused by customer-authorized requests, commands, API calls, scope decisions, credentials, or instructions.

Customer has read and accepts this limitation of liability and waiver.

NEURALBYTES CUSTOMER-CONTROLLED WORKFLOW AGREEMENT

Partner terms, API access, payment, and prohibited use

Page 5 of 6

PART L Partner and Referral Terms

If this agreement is used by a partner or referral source, Partner confirms authority to request bridge access or introduce the end customer. Partner must not promise guaranteed outcomes, must not misrepresent NeuralBytes, and must obtain customer consent before requesting agent, API, remote access, or automation workflows. Referral fees, revenue share, reseller terms, white-label terms, and API access require separate written approval.

Not applicable; direct customer agreement.

Partner/referral terms apply and are accepted.

PART M Payment and Cancellation

BILLING FREQUENCY

PAYMENT DUE DATE

CANCELLATION NOTICE

NeuralBytes may pause or terminate bridge/API access for nonpayment, abuse, unlawful activity, unsafe requests, unauthorized access requests, security concerns, or work outside the approved scope. Customer remains responsible for approved charges incurred before cancellation.

PART N Authorized Use, API Access, and Prohibited Activity

Customer may not use NeuralBytes tools, agents, bridge access, automation, or API access for unauthorized access, malware, spam, credential theft, surveillance without consent, evasion of security controls, or unlawful activity. API access, if granted, may be limited, monitored, rate-limited, revoked, and subject to additional written terms. Customer is responsible for requests sent through approved credentials.

Customer accepts authorized-use restrictions, API access limits, and credential responsibility.

PART O Confidentiality and Records

NeuralBytes will use reasonable care with customer information observed through the bridge, agent, API, or support process. Records may be retained as reasonably needed for service history, troubleshooting, security review, legal compliance, billing, and business operations.

CUSTOMER RECORD RETENTION OR CONFIDENTIALITY NOTES

NEURALBYTES CUSTOMER-CONTROLLED WORKFLOW AGREEMENT

Electronic signature and final acceptance

Page 6 of 6

PART P Electronic Signature Consent

Customer agrees that a handwritten signature, electronic signature, typed name, checkbox, submitted form, invoice payment, or electronically stored acceptance record may show acceptance where permitted by law. Customer agrees to receive and retain this agreement electronically.

- Customer consents to electronic records and electronic signatures.
- Customer requests a printed copy.

PART Q Incorporated Documents

By signing, submitting, checking an agreement box, paying an invoice, using API credentials, launching an agent, or allowing a session to begin, Customer accepts this Customer-Controlled Workflow Agreement, the NeuralBytes End User Agreement, the NeuralBytes Privacy Policy, and any written access scope or invoice terms applicable to the work.

PART R Final Signatures

CUSTOMER / PARTNER SIGNATURE

DATE

PRINTED NAME

TITLE / AUTHORITY

NEURALBYTES REPRESENTATIVE

DATE

COPY RETENTION

Customer should keep a signed copy. NeuralBytes should store the signed agreement with the customer record, invoice, workflow request, support ticket, or CRM entry.