CYBERHOOT TERMS OF SERVICE

Effective Date: *July 8th, 2026*

PREAMBLE AND ACCEPTANCE

These Terms of Service ("Terms" or "Agreement") govern your access to and use of CyberHoot, LLC's cybersecurity awareness learning management platform, phishing simulation system, automation tools, websites (including cyberhoot.com and its subdomains), email-delivered training, and all related services ("Service"). By clicking "I Agree," creating an Account, or accessing the Service, you accept these Terms and form a binding contract with CyberHoot, LLC ("CyberHoot," "we," "us," or "our").

If you do not accept these Terms, do not access the Service. If you are using the Service on behalf of a company or organization, you represent and warrant that you have authority to bind that entity to these Terms. This Agreement applies to all Customers worldwide, including those using CyberHoot directly or through a Partner (including managed service providers and resellers).

1. DEFINITIONS

"**Account**" means your registered login credentials, subscription details, and associated data.

"**Confidential Information**" means non-public information disclosed by either party, including source code, algorithms, security practices, business plans, pricing, and personal data, that is marked confidential or reasonably identifiable as such.

"**Customer Data**" means data uploaded by Customer or its users into the Service, including personal data processed on behalf of Customer.

"End-Customer" means a downstream client of a Partner for whom the Partner administers CyberHoot Services under Section 18.

"Feedback" means suggestions, ideas, or comments provided by Customer regarding the Service.

"**Partner"** means a Customer authorized to administer CyberHoot for multiple downstream clients under Section 18, including Managed Service Providers (MSPs) and resellers.

"**Service**" means CyberHoot's cybersecurity awareness training platform, phishing simulations, automation tools, and related services.

2. ACCEPTABLE USE AND RESTRICTIONS

You shall use the Service only in compliance with applicable law and this Agreement. You shall not:

(1) Train artificial intelligence, machine learning models, or large language models using the Service, its outputs, or its data without express written consent;
(2) Circumvent or disable security features, authentication mechanisms, or access controls;
(3) Upload malicious code or engage in denial-of-service attacks;
(4) Scrape, spider, or systematically extract data from Service except through authorized APIs;
(5) Resell or redistribute the Service without authorization under Section 18;
(6) Use the Service to transmit unlawful, discriminatory, or harmful content; or
(7) Use the Service in violation of export control laws, sanctions, or embargoes.

IP-related restrictions including reverse engineering, derivative works, competitive analysis, and replication are governed by Section 4.2. CyberHoot may suspend or terminate access immediately for violations of this section.

3. LICENSE GRANT and API Access

3.1 Service License

CyberHoot grants you a limited, non-exclusive, non-transferable, revocable license to use the Service solely for internal business use or, for Partners, internal use plus administration of downstream clients as permitted under Section 18. You receive no rights to source code, algorithms, phishing simulation logic, reinforcement methodology, or platform-generated insights except as required for use of the Service.

3.2 API Access and Restrictions

Customer and authorized users may access CyberHoot APIs and integrations as enabled through account configuration, API key issuance, or platform provisioning. No separate written authorization is required.

3.3 Monitoring and Revocation Rights

API access is limited to use in connection with the Service and Customer-managed integrations and workflows. CyberHoot may monitor, rate limit, suspend, or revoke API access at any time for security risk, misuse, excessive load, competitive activity, or operational risk.

API access does not grant any ownership or license rights beyond use of the Service. API documentation, schemas, scoring logic, and platform behavior constitute CyberHoot Confidential Information.

4. INTELLECTUAL PROPERTY AND OWNERSHIP

CyberHoot retains all right, title, and interest in the Service and all derivative works, including but not limited to: the HootPhish positive reinforcement methodology and all associated gamification, behavioral, and scoring systems. Nothing in this Agreement transfers ownership to Customer.

CyberHoot is actively pursuing U.S. patent protection for its methodologies. All patent-pending methodologies, workflow designs, automation logic, and system architecture constitute Confidential Information. Customer agrees not to intentionally design around CyberHoot's disclosed patent claims using knowledge gained from access to the Service. This does not prohibit independently developed non-infringing solutions using publicly available information.

4.1 Feedback

You may provide feedback regarding the Service. You grant CyberHoot a non-exclusive, worldwide, perpetual, irrevocable, royalty-free license to use and incorporate any feedback into the Service, including any pre-existing intellectual property you disclose. Do not include proprietary information unless you intend to grant these rights, as you cannot revoke CyberHoot's license once provided. You represent that you own or have rights to provide all feedback.

4.2 IP Use Restrictions

Customer shall not, directly or indirectly: (a) reverse engineer, disassemble, or derive source code or methodology; (b) use Service to develop or inform competing products, including through competitive analysis, benchmarking, AI/ML training, or insights derived from Service; (c) copy, replicate, or create derivative works; (d) capture system behavior for replication; or (e) design around disclosed patent claims using knowledge gained from Service access. These restrictions apply regardless of access method (UI, API, export, integration).

5. CUSTOMER DATA, PRIVACY, AND DATA PROCESSING

5.1 Data Processing Framework

Customer grants CyberHoot a limited license to use Customer Data solely for providing and improving the Service. CyberHoot receives no ownership of Customer Data. Customer represents that Customer Data does not infringe third-party rights. Customer ("**Data Controller**") provides Customer Data to CyberHoot ("**Data Processor**"). CyberHoot processes Customer Data solely as instructed by Customer and for service delivery, security (including fraud and misuse prevention), and platform improvement.

For free individual accounts (non-commercial use), the individual user is the Data Controller and CyberHoot processes personal data to provide the Service directly to the user under this Agreement. The data processing provisions in this Section 5 apply, with "Customer" understood to mean the individual user.

CyberHoot does not sell Customer Data or use it for third-party targeted advertising.

For employer-sponsored accounts, this section constitutes a Data Processing Addendum as required by GDPR Articles 28-32. CyberHoot processes data solely on behalf of Customer. Customer is responsible for ensuring accuracy and legality of Customer Data, obtaining required consents, and complying with applicable privacy laws.

For free individual accounts, CyberHoot may send product-related communications (service updates, upgrade offers, educational content). You may opt out of promotional emails at any time while continuing to receive service-critical notifications.

5.2 Data Hosting, Categories, and International Transfers

CyberHoot processes minimal personal data: names, email addresses, role information, company hierarchy, training results, IP address, administrator authentication data (login credentials, MFA data including phone numbers if SMS MFA is enabled, and passkey credentials when supported), and (if enabled) dark web monitoring data consisting of email addresses, domains, and redacted credential fragments.

CyberHoot does not process or store: Social Security numbers, payment card data, biometric data, or health data. Customer should not upload such data unless required for legitimate purposes.

For Customers subject to GDPR, UK GDPR, or Swiss data protection laws:

(a) Standard Contractual Clauses and other appropriate safeguards are available upon request. Contact dpo@cyberhoot.com to execute required documentation.
(b) If Customer does not request SCCs, Customer represents that: (i) it has an alternative lawful basis for transferring personal data to the United States, and (ii) it has fulfilled all obligations required under applicable data protection law for such transfer.
Customer acknowledges CyberHoot processes personal data in the United States as necessary to deliver the Service.

CyberHoot is addressing its GDPR Article 27 obligations regarding EU/UK representative appointment. In the interim, Customers subject to GDPR, UK GDPR, or Swiss data protection law may direct inquiries to dpo@cyberhoot.com.

5.3 Subprocessors

We engage vetted subprocessors to deliver the Service. All subprocessors are contractually bound to equivalent data protection obligations.

A current list is available to administrators inside the CyberHoot platform for partner and/or client review. We provide 30 days' advance notice for new subprocessors through the platform, not by public posting. Your employer may object within 15 days by contacting dpo@cyberhoot.com. If we cannot provide an alternative, your employer may terminate without penalty.

5.4 Security Incident and Data Breach Notification

CyberHoot will notify Customer without undue delay upon confirming a material Security Incident involving unauthorized access to Customer Data. For EU/UK/Swiss data subjects, notification within 72 hours of a confirmed incident. For U.S. residents, within the timeframe required by applicable state breach notification laws. Notification via email to Customer's designated administrative contact. Customer is responsible for providing required notices to affected individuals and regulators unless applicable law expressly requires CyberHoot to do so directly.

5.5 Data Subject Rights

CyberHoot will assist Customer in responding to reasonably verified and identity-validated data subject requests (access, correction, deletion, restriction, portability) within 30 calendar days of Customer's request for assistance. CyberHoot does not respond to data subject requests directly unless legally required.

5.6 Data Retention and Deletion

Customer Data is retained during the subscription term. Upon termination, Customer may export data for 30 days. After 30 days, CyberHoot may securely delete Customer Data using industry-standard destruction methods. Legal holds may extend retention as required by law.

5.7 Security Measures

CyberHoot implements commercially-reasonable security controls including: encryption in transit and at rest; multi-factor authentication for administrators; intrusion detection; annual penetration testing; regular vulnerability scanning; role-based access control; and secure software development lifecycle (SDLC).

Customer is responsible for: enabling MFA; maintaining strong unique passwords (15+ characters minimum); timely user provisioning and deprovisioning; and securing devices used to

access CyberHoot. Administrator accounts require password authentication or passkey authentication (when supported) and should be protected with multi-factor authentication.

API Credential Security: Customer must protect API credentials using commercially reasonable security controls and restrict access to authorized personnel. Customer must promptly rotate compromised API credentials and notify CyberHoot without unreasonable delay, and no later than 72 hours after confirming an API-related security incident.

6. Confidentiality

Each party will maintain the other's Confidential information in confidence using the same standard of care it uses for its own confidential information (but no less than reasonable care), limit access to personnel with a need to know, and not disclose to third parties without written consent.

Exceptions: information that is (a) publicly available through no fault of the recipient, (b) rightfully known prior to disclosure, (c) independently developed, or (d) required to be disclosed by law (with prior written notice when permitted).

Confidentiality obligations survive termination for five years.

7. DARK WEB MONITORING

CyberHoot's dark web monitoring scans publicly accessible dark web sources for credential exposures on a best-efforts basis. Customer acknowledges:

(a) CyberHoot does not guarantee detection of all exposures, cannot verify source authenticity, and results may include false positives or reflect historical rather than real-time data;
(b) CyberHoot provides redacted password information only and does not store plaintext passwords;
(c) Customer is solely responsible for determining response actions, validating credentials, enforcing password changes, and notifying users.
Dark web monitoring is a supplemental awareness tool and does not replace password policies, MFA, or other security controls. Liability limitations in Section 11 apply.

8. FEES, BILLING, AND CANCELLATION

Subscriptions are month-to-month or annual prepayment. Monthly subscriptions auto-renew unless cancelled; customers may cancel at any time with no refund for the remaining billing period. Annual prepayments are non-refundable for the prepaid term. CyberHoot may adjust pricing with 60 days' advance notice; adjustments do not apply to annual prepayments until the next renewal term.

9. SUPPORT AND AVAILABILITY

CyberHoot provides support via email (support@cyberhoot.com), knowledge base (support.cyberhoot.com), and in-platform AI chatbot. Support response targets are typically within 24 business hours, but not guaranteed. CyberHoot will use commercially reasonable efforts to maintain 99.5% uptime monthly, excluding scheduled maintenance and Force Majeure Events. Enterprise SLA tiers with guaranteed response times are available by separate agreement.

Customer's sole remedy for failure to meet the 99.5% uptime commitment is a service credit equal to the pro-rated fees for the hours of verified downtime exceeding the monthly threshold, up to a maximum of one month's fees. Credits must be requested within 30 days of the incident and are applied to future invoices. Credits do not apply during Force Majeure Events or scheduled maintenance.

10. WARRANTY DISCLAIMERS

THE SERVICE IS PROVIDED 'AS-IS' WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. CyberHoot provides cyber literacy training, not security guarantees, breach prevention, compliance certification, or definitive cybersecurity advice. CyberHoot does not warrant error-free or uninterrupted service, specific risk reduction outcomes, or that training prevents attacks.

Phishing simulations are educational tools. Customer is responsible for user notification, reasonable accommodations, and not basing adverse employment actions solely on simulation results. Completion records do not constitute regulatory compliance certification.

11. LIMITATION OF LIABILITY

CYBERHOOT'S TOTAL AGGREGATE LIABILITY SHALL NOT EXCEED THE LESSER OF (A) SIX MONTHS OF FEES PAID OR (B) $10,000. CYBERHOOT SHALL NOT BE LIABLE FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES, INCLUDING LOST PROFITS, REVENUE, BUSINESS INTERRUPTION, REPUTATIONAL HARM, OR COST OF SUBSTITUTE SERVICES, EVEN IF ADVISED OF THE POSSIBILITY, OR DAMAGES ARISING FROM FORCE MAJEURE EVENTS.

These limitations do not apply to: (A) CyberHoot’s indemnification obligations, which remain capped at six (6) months of fees paid; (B) claims arising from gross negligence or willful misconduct; or (C) liabilities that cannot be limited under applicable law, including GDPR Article 82 liability, statutory consumer protection violations, and fraudulent misrepresentation.

Security Breach Clarification: Liability limitations apply to breaches caused by third-party attacks where CyberHoot has implemented commercially reasonable and industry-aligned security measures appropriate to the nature of the Service and data processed.

12. INDEMNIFICATION

12.1 Customer Indemnity

Customer agrees to indemnify and defend CyberHoot against claims arising from misuse of the Service, violation of law, Customer Data infringement, Partner or downstream client misuse, and employment-related claims arising from Customer's use of phishing simulations or training results.

12.2 CyberHoot Indemnity

CyberHoot will indemnify, defend, and hold Customer harmless from third-party claims that the Service, as provided by CyberHoot and used in accordance with this Agreement, directly infringes a valid U.S. patent, copyright, or trademark, or results from CyberHoot's material breach of its data processing obligations under this Agreement, limited to provable direct damages.

CyberHoot shall have no indemnity obligation to the extent a claim arises from: (i) Customer modifications; (ii) use outside the permitted scope; (iii) combination with non-CyberHoot products or data; (iv) Customer Data; (v) use after CyberHoot provides a non-infringing replacement; or (vi) Customer or End-Customer configuration, security practices, or administrative actions.

CyberHoot's total liability under this indemnification shall not exceed the liability cap set forth in Section 11, except for GDPR Article 82 claims which cannot be contractually limited.

CyberHoot shall control the defense and settlement of any claim, provided that it will not settle any claim imposing non-monetary obligations on Customer without Customer's prior written consent (not to be unreasonably withheld). Customer shall provide reasonable cooperation at CyberHoot's expense.

13. INSURANCE

CyberHoot maintains commercially reasonable insurance coverage including technology errors and omissions liability and cyber liability coverage. Upon written request, CyberHoot will provide a certificate of insurance. CyberHoot may update its policies provided coverage remains commercially reasonable. Insurance is maintained for CyberHoot's benefit and does not create additional Customer rights.

14. SUSPENSION AND TERMINATION

CyberHoot may suspend or terminate access for: non-payment; security threats; abuse or violation of this Agreement; legal requirements; or prolonged Force Majeure Events.

Data retention and deletion upon termination are governed by Section 5.6.

14.1 Survival

Confidentiality, IP rights, indemnification, liability limitations, dispute resolution, and governing law survive termination.

15. DISPUTE RESOLUTION AND GOVERNING LAW

This Agreement is governed by the laws of the State of Delaware. Except for IP disputes requiring injunctive relief or collection of unpaid fees, all disputes must be resolved by binding arbitration through the American Arbitration Association (AAA) in Delaware, USA. The arbitration decision is final and enforceable.

CLASS ACTION WAIVER: EXCEPT WHERE PROHIBITED BY LAW, ALL DISPUTES SHALL BE RESOLVED ON AN INDIVIDUAL BASIS, NOT AS A CLASS ACTION, CLASS ARBITRATION, OR REPRESENTATIVE PROCEEDING. EACH PARTY WAIVES THE RIGHT TO PARTICIPATE IN CLASS ACTIONS. IF THIS WAIVER IS FOUND UNENFORCEABLE, IT SHALL BE SEVERED AND THE REMAINING ARBITRATION PROVISIONS ENFORCED.

EACH PARTY WAIVES THE RIGHT TO A JURY TRIAL.

CyberHoot is entitled to seek injunctive relief without posting bond for breaches of IP, confidentiality, or acceptable use provisions.

16. FORCE MAJEURE

Neither party is liable for failure to perform obligations (except payment) due to events beyond reasonable control, including natural disasters, war, terrorism, pandemics, government actions, or critical infrastructure attacks, provided notice within 5 days and reasonable mitigation efforts. Force Majeure excludes events within the party's reasonable control. If Force Majeure prevents service delivery beyond 60 consecutive days, either party may terminate without penalty. Payment, confidentiality, data protection, and IP obligations continue.

17. MODIFICATIONS

CyberHoot may update these Terms from time to time. The current version will be posted at cyberhoot.com and will become effective upon posting unless otherwise stated.

For material changes that substantially affect Customer rights, data processing practices, or liability limitations, CyberHoot will use commercially reasonable efforts to provide notice via email or in-platform notification. Continued use of the Service after the effective date constitutes acceptance of the updated Terms.

18. PARTNER TERMS

This section applies to Customer administering CyberHoot for multiple downstream clients ("End-Customer").

Customer may administer CyberHoot Services on behalf of End-Customer subject to compliance with this Agreement, acceptance of brand use requirements, and payment of applicable pricing.

Restrictions: Customer may not white-label or rebrand except where CyberHoot explicitly provides white-labeling functionality within the Platform or within related materials (infographics, whitepapers). Customer may not create derivative versions of workflows, simulations, or reinforcement models; misrepresent themselves as CyberHoot employees; market competing platforms using CyberHoot materials; or build competitive products using insights from CyberHoot.

Responsibilities: Customer is responsible for accurate End-Customer tenant setup, billing relationships, first-line support, ensuring End-Customer TOS compliance, and security of accounts and credentials. Customer represents they have obtained consent from End-Customer to manage their data.

Partner-Specific Terms: Customer indemnifies CyberHoot for claims arising from misconfiguration, unauthorized access, misrepresentations, and violations by Customer or End-Customer. CyberHoot may suspend or terminate Partner privileges for non-payment, abuse, security risks, systematic TOS violations, or negligent misconfigurations. Customer must notify End-Customer before terminating service. General indemnification, liability, and termination provisions in Sections 12-13 and 15 apply to Partners.

19. EDUCATION SECTOR COMPLIANCE

FERPA

For institutions subject to FERPA (20 U.S.C. Section 1232g), CyberHoot acts as a "School Official" with legitimate educational interest. CyberHoot will use education records solely for authorized training purposes, not disclose them without Customer consent, maintain FERPA-required safeguards, and return or destroy records upon request.

COPPA and Minors' Privacy

CyberHoot does not collect personal information directly from users known to be under 13 (US/COPPA) or under 16 (EU/UK/GDPR). Customer warrants that no users under 13 will be provisioned without parental consent, and that no users between 13 and 16 in GDPR jurisdictions will be provisioned without verifiable parental or guardian consent as required under GDPR Article 8. If CyberHoot discovers underage users provisioned without proper consent, it will notify Customer and suspend affected accounts pending Customer's resolution.

Student Privacy

For K-12 Customer, CyberHoot commits to the Student Privacy Pledge principles and, for California K-12 Customer, will not use student data for targeted advertising or non-educational profiling.

20. GENERAL PROVISIONS

Entire Agreement. This Agreement constitutes the entire agreement between the parties and supersedes all prior negotiations, understandings, and agreements.

Severability. If any provision is found unenforceable, it shall be modified to the minimum extent necessary or severed; remaining provisions continue in full force.

Waiver. No waiver is effective unless in writing. Failure to enforce a right does not constitute waiver.

Assignment. Customer may not assign without CyberHoot's consent. CyberHoot may assign to an affiliate or successor without consent.

No Partnership. This Agreement does not create a partnership, joint venture, or agency relationship.

Notices. Legal notices to CyberHoot: dpo@cyberhoot.com. Support: support@cyberhoot.com. Current terms: cyberhoot.com.

Audit Rights. Upon reasonable written notice and execution of a mutually agreed non-disclosure agreement, Customer may request compliance documentation including SOC 2 summaries and penetration testing summaries. CyberHoot will provide such documentation within a commercially reasonable timeframe.

Interpretation. "Including" means "including without limitation." Headings are for convenience only.

END OF TERMS OF SERVICE