INFILTRATEIQ TERMS AND CONDITIONS

Last Updated: February 9, 2026

By accessing and using Infiltrate ("the Service"), you ("User") acknowledge that you have read, understood, and agree to be bound by these Terms and Conditions ("Agreement"). If you do not agree with any part of this Agreement, you are prohibited from using the Service.

This Agreement constitutes the entire agreement between you and InfiltrateIQ Inc. ("Infiltrate," "We," or "Us,") regarding the use of the Service and supersedes all prior or contemporaneous communications and proposals.

You affirm that you are more than 18 years of age, or an emancipated minor, or possess legal parental or guardian consent, and are fully able and competent to enter into the terms, conditions, obligations, affirmations, representations, and warranties set forth in these Terms and Conditions.

1. Definitions

"Confidential Information" means any written, electronic, or oral information provided or disclosed by one party (the "Disclosing Party") to the other party (the "Receiving Party") that is clearly marked or identified as "confidential" or "proprietary," or that a reasonable person would understand to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information includes, without limitation, technical data, trade secrets, know-how, research, product plans, software, services, customers, markets, developments, inventions, processes, formulas, technology, designs, drawings, engineering, marketing, finances, Penetration Test results, vulnerability reports, and other business information.

"Private Information" means consumer, customer, or individual information that may be subject to the protections of federal, provincial, state, and/or local privacy, safeguards, or information security laws, including but not limited to names, addresses, financial information, and any other personally identifiable information.

"Target Environment" means the website, application, network, system, or other digital infrastructure that User submits to the Service for Penetration Testing.

"Penetration Test" means automated penetration testing, vulnerability identification, exploitation validation, security audits, and related security evaluation activities performed by the Service.

"Affiliate" means with respect to a party, any entity that, directly or indirectly, is controlled by, controls, or is under common control with such party. "Control" means the possession, directly or indirectly, of the power to direct or cause the direction of management or policies, whether through ownership of voting securities, by contract, or otherwise.

2. Service Description

Infiltrate offers an automated platform designed to conduct Penetration Tests of Target Environments. The Service utilizes various tools and techniques to identify potential security vulnerabilities and weaknesses.

The Service is intended to provide an overview of potential security issues and is not a comprehensive assessment of all security aspects of the Target Environment. The effectiveness of the Service is dependent on the accuracy and completeness of the information provided by User.

Infiltrate reserves the right to modify, suspend, or discontinue the Service or any part of it at any time with reasonable notice to active Users. This includes updates and improvements to the Service, as well as changes in the tools, techniques, and methodologies used to perform Penetration Tests.

AI-Driven Testing: Automated Service. The Service utilizes Infiltrate's proprietary artificial intelligence system ("Vana") to perform Penetration Tests. By default, all testing, analysis, vulnerability identification, and report generation are performed entirely by Vana without human review or intervention. This AI-only approach is designed to protect User's privacy and ensure consistent, rapid delivery of results.

AI-Driven Testing: Optional Human Review. Upon User's written request, Infiltrate can arrange for qualified security professionals to review Vana's findings and reports. Human review services may be subject to additional fees, extended delivery timelines, and a separate statement of work. User acknowledges that requesting human review means Infiltrate personnel will access User's Confidential Information, including vulnerability findings and Target Environment details.

AI-Driven Testing: Privacy Consideration. User acknowledges that electing AI-only testing (the default) means no Infiltrate employee or contractor will view User's Penetration Test results, Target Environment information, or vulnerability reports unless User explicitly authorizes human review or unless required by law.

AI Limitations: No Perfect Solution. User acknowledges that no penetration testing methodology—whether AI-driven or human-performed—can guarantee the detection of all vulnerabilities or the absence of false findings. Vana is designed to identify a broad range of security issues, but like any testing approach, it has inherent limitations.

AI Limitations: Potential for Errors. AI-driven Penetration Tests may produce false positives (identifying issues that do not exist or are not exploitable) or false negatives (failing to detect vulnerabilities that exist). User is responsible for validating findings and exercising professional judgment before implementing remediation measures.

AI Limitations: Complementary Security Measures. The Service is intended to be one component of User's overall security program. Infiltrate recommends that Users maintain additional security controls, conduct periodic manual assessments as appropriate, and not rely solely on any single testing methodology—AI or otherwise.

AI Limitations: Evolving Threat Landscape. Cyber threats evolve continuously. Vana is regularly updated to address emerging vulnerabilities and attack techniques, but there may be a delay between the emergence of new threats and Vana's ability to detect them. A clean Penetration Test result does not guarantee ongoing security.

3. User Obligations and Authorization

Authorization Requirement. User represents and warrants that User is the lawful owner of, or has obtained express written authorization from the lawful owner of, the Target

Environment to be tested. Upon request, User shall provide Infiltrate with documentation evidencing such ownership or authorization.

Scope Definition. Prior to commencement of any Penetration Test, User shall provide Infiltrate with a written scope document specifying: (i) the Target Environment(s) authorized for testing; (ii) the testing window (dates and times); (iii) any systems, data, or functionality explicitly excluded from testing; (iv) permitted testing techniques; and (v) emergency contact information.

Compliance with Laws. User shall comply with all applicable local, provincial, state, national, and international laws, rules, and regulations in connection with User's use of the Service. User shall not use the Service for any illegal purposes or in any manner that would violate the rights of third parties.

Production Environment Testing. User agrees to use the Service on non-production environments unless User has expressly elected to test production environments and accepts the associated risks as set forth in Section 8 (Production Testing Risks). In all cases, User acknowledges that Penetration Tests may cause service degradation, denial-of-service conditions, data loss, or other disruptions, and User assumes responsibility for implementing appropriate safeguards and backup procedures.

Account Security. User is responsible for maintaining the confidentiality of account information, including passwords, and for all activities that occur under User's account. User agrees to immediately notify Infiltrate of any unauthorized use of User's account or any other breach of security.

Responsible Disclosure. If User discovers any security-related issues or vulnerabilities related to the Service itself, User agrees to responsibly report these issues to Infiltrate as soon as possible at spencer.fairbairn@infiltrateiq.com.

4. Confidentiality

Mutual Confidentiality Obligations. Each party agrees to hold in confidence all Confidential Information of the other party and to use such Confidential Information only for the purposes of this Agreement. Each party shall protect the other party's

Confidential Information using the same degree of care it uses to protect its own confidential information, but in no event less than reasonable care.

User Confidential Information. Infiltrate acknowledges that information submitted by User to the Service, including but not limited to Target Environment details, vulnerability reports, security assessment results, and any Private Information accessed during testing, constitutes User's Confidential Information. Infiltrate shall not disclose, publish, or otherwise disseminate User's Confidential Information to any third party without User's prior written consent.

Permitted Disclosures. Each party may disclose Confidential Information to its employees, contractors, Affiliates, attorneys, auditors, and financial advisors on a need-to-know basis, provided such recipients are bound by confidentiality obligations no less protective than those contained herein.

Exceptions. Confidential Information shall not include information that: (i) is or becomes publicly available without breach of this Agreement; (ii) was known to the Receiving Party prior to disclosure; (iii) is received from a third party without breach of any confidentiality obligation; or (iv) is independently developed by the Receiving Party without use of the Disclosing Party's Confidential Information.

Compelled Disclosure. If the Receiving Party is required to disclose Confidential Information pursuant to any legal process or governmental order, the Receiving Party shall: (i) promptly notify the Disclosing Party so that the Disclosing Party may seek a protective order or other appropriate remedy; (ii) comply with any applicable protective order; and (iii) disclose only that portion of the Confidential Information that is legally required to be disclosed.

Return or Destruction. Upon termination of this Agreement or upon the Disclosing Party's written request, the Receiving Party shall promptly return or destroy all Confidential Information and certify such return or destruction in writing.

Survival. The confidentiality obligations under this Section 4 shall survive termination or expiration of this Agreement for a period of three (3) years; provided, however, that obligations with respect to Private Information shall survive indefinitely.

5. Privacy and Data Protection

Data Collection. When User uses the Service, Infiltrate may collect personal information that User provides, such as name, contact information, and Target Environment details. Additionally, Infiltrate may collect information about User's usage of the Service, including traffic data and location data.

Data Use. Information collected is used to provide, maintain, and improve the Service, to personalize User's experience, and to communicate with User about the Service. Infiltrate may also use aggregated, anonymized data for internal purposes such as auditing, data analysis, and research to improve Infiltrate's products and services.

No Sale of Data. Infiltrate will not sell, rent, or lease User's personal information or Confidential Information to third parties.

Security Measures. Infiltrate implements reasonable security measures, including encryption and secure server hosting, to safeguard the confidentiality of User's information. Infiltrate shall encrypt Confidential Information and Private Information at rest and in transit.

Canadian Privacy Law Compliance. Infiltrate processes personal information in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy legislation. For Users located outside Canada, Infiltrate shall also comply with applicable data protection laws in User's jurisdiction to the extent required, including but not limited to the General Data Protection Regulation (GDPR) for Users in the European Economic Area and the California Consumer Privacy Act (CCPA) for Users in California.

Private Information Compliance. Both parties acknowledge that Private Information may be subject to the protections of federal, provincial, state, and/or local privacy laws. Each party agrees to comply with all applicable data protection laws with respect to any Private Information accessed or processed in connection with this Agreement.

Data Subject Rights. User may have rights to access, correct, update, or delete personal information that Infiltrate holds, in accordance with PIPEDA and other applicable privacy laws. To exercise these rights, User may contact Infiltrate at privacy@infiltrateiq.com.

Data Retention for Retesting: Retention Period. To enable retest functionality, Infiltrate may retain User's custom testing instructions, configuration settings, scope parameters, and related assessment data ("Retest Data") for up to ninety (90) days following the completion of a Penetration Test.

Data Retention for Retesting: Purpose Limitation. Retest Data is retained solely to allow User to initiate follow-up Penetration Tests using the same parameters and custom instructions as prior tests. Infiltrate shall not use Retest Data for any other purpose without User's prior written consent.

Data Retention for Retesting: Security. Retest Data is stored using the same security measures applied to Confidential Information as described in this Section 5, including encryption at rest and in transit.

Data Retention for Retesting: Deletion. Upon expiration of the ninety (90) day retention period, Retest Data shall be automatically deleted. User may request earlier deletion of Retest Data at any time by contacting Infiltrate at privacy@infiltrateiq.com, in which case Infiltrate shall delete such data within ten (10) business days. User acknowledges that early deletion will disable retest functionality for the applicable Penetration Test.

6. Indemnification

User Indemnification. User shall indemnify, defend, and hold harmless Infiltrate and its Affiliates, officers, directors, employees, and agents from and against any third-party claims arising from: (i) User's use of the Service without proper authorization for the Target Environment; (ii) User's violation of applicable laws; (iii) User's intentional or negligent unauthorized disclosure or misuse of Infiltrate's Confidential Information; or (iv) User's violation of applicable data protection laws with respect to Private Information.

Infiltrate Indemnification. Infiltrate shall indemnify, defend, and hold harmless User and its Affiliates, officers, directors, employees, and agents from and against any third-party claims arising from: (i) Infiltrate's intentional or negligent unauthorized disclosure or misuse of User's Confidential Information; (ii) Infiltrate's violation of applicable data protection laws with respect to Private Information; or (iii) Infiltrate's gross negligence or willful misconduct in performing the Service.

Indemnification Procedures. The indemnified party shall: (i) promptly notify the indemnifying party of any claim; (ii) allow the indemnifying party to control the defense and settlement of such claim; and (iii) provide reasonable cooperation at the indemnifying party's expense. The indemnifying party shall not settle any claim without the indemnified party's prior written consent, which shall not be unreasonably withheld.

Limitation. Neither party shall indemnify the other for the other party's own negligence or willful misconduct.

Survival and Claims Period. Indemnification obligations shall survive termination of this Agreement for a period of two (2) years. Any claim for indemnification must be asserted in writing within one (1) year after the indemnified party becomes aware of the facts giving rise to such claim, but in no event later than two (2) years after termination of this Agreement. Failure to provide timely notice shall not relieve the indemnifying party of its obligations except to the extent the indemnifying party is materially prejudiced by such delay.

7. Limitation of Liability

Liability Cap. Except for breaches of Section 4 (Confidentiality), violations of applicable data protection laws with respect to Private Information, or a party's indemnification obligations under Section 6, each party's aggregate liability under this Agreement shall not exceed the greater of: (i) CAD $100,000; or (ii) the total fees paid by User to Infiltrate in the twelve (12) months preceding the claim.

Exclusion of Consequential Damages. Neither party shall be liable for any indirect, incidental, special, consequential, or punitive damages, including without limitation loss of profits, data, use, goodwill, or other intangible losses, whether based on warranty, contract, tort (including negligence), or any other legal theory, even if advised of the possibility of such damages.

Exceptions. The limitations in Section 7(b) shall not apply to: (i) a party's breach of Section 4 (Confidentiality); (ii) a party's violation of applicable data protection laws; (iii) a party's gross negligence or willful misconduct; or (iv) User's use of the Service without proper authorization.

Service Interruptions. Infiltrate does not guarantee that the Service will function without interruption or errors. The Service may be interrupted due to maintenance, updates, or system or network failures. Infiltrate shall use reasonable efforts to provide advance notice of planned maintenance.

No Warranty. The Service is provided "as is" and "as available." Infiltrate makes no representations or warranties as to the accuracy, completeness, or reliability of the Service or any Penetration Test results. User acknowledges that no Penetration Test can guarantee detection of all vulnerabilities.

Time Limitation on Claims. Liability under this Agreement is limited to events occurring during the term of this Agreement or the two (2) year survival period following termination. Any claim arising under or relating to this Agreement must be brought within two (2) years of the event giving rise to such claim, regardless of when the claiming party became aware of such event. This limitation shall apply to the fullest extent permitted by applicable law.

8. Production Testing Risks

Acknowledgment of Risk. User understands that Penetration Tests of production environments may cause service degradation, denial-of-service conditions, data loss, unintended communications, rate-limit restrictions, or other disruptions to the Target Environment.

Safe Testing Practices. Infiltrate shall use industry-standard safe testing practices and shall avoid intentional service disruption or exfiltration of Private Information beyond what is necessary to demonstrate vulnerabilities. Testing shall be conducted within the scope, timing, and permitted techniques specified by User.

User Preparation. User is responsible for: (i) ensuring no modifications are made to the Target Environment during the testing period that could interfere with testing; (ii) ensuring adequate resources are available to handle testing load; (iii) implementing appropriate backup and recovery procedures; and (iv) designating personnel to respond to any issues during testing.

Testing Interruptions. Either party may suspend testing at any time if the testing causes or threatens to cause material disruption to the Target Environment or any third-party systems. Such suspension shall not constitute a breach of this Agreement, and the parties shall work together in good faith to resolve the issue and resume testing if appropriate.

9. Intellectual Property

Infiltrate IP. All content on the Service, including but not limited to text, graphics, logos, images, software, and the compilation thereof, is the exclusive property of Infiltrate or its licensors and is protected by applicable intellectual property laws. Nothing in this Agreement grants User any license to Infiltrate's intellectual property except the limited right to use the Service as contemplated herein.

User IP. User retains all rights in User's Confidential Information and any intellectual property contained therein. Infiltrate acquires no ownership interest in User's intellectual property through the provision of the Service.

Feedback. If User provides feedback, suggestions, or ideas regarding the Service, Infiltrate may use such feedback without obligation to User; provided, however, that such feedback shall not include User's Confidential Information unless User expressly authorizes such use in writing.

10. Term and Termination

Term. This Agreement shall become effective upon User's acceptance and shall continue until terminated as provided herein.

Termination for Convenience. Either party may terminate this Agreement at any time upon thirty (30) days' written notice to the other party.

Termination for Cause. Either party may terminate this Agreement immediately upon written notice if the other party materially breaches this Agreement and fails to cure such breach within fifteen (15) days after receiving written notice thereof.

Effect of Termination. Upon termination, User shall cease using the Service, and each party shall return or destroy the other party's Confidential Information as provided in Section 4. Sections 4, 5, 6, 7, 9, 11, 12, and 13 shall survive termination.

11. Governing Law and Dispute Resolution

Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein, without regard to conflict of law principles. Notwithstanding the foregoing, where the parties have executed a mutual non-disclosure agreement that specifies governing law and dispute resolution provisions, those provisions shall take precedence over this Section 11 to the extent of any inconsistency.

Global Service; Consent to Jurisdiction. User acknowledges that the Service is operated from Ontario, Canada, and that this Agreement shall be governed by Ontario law regardless of User's location. By using the Service, User expressly consents to the exclusive jurisdiction of the courts of Ontario, Canada, and waives any objection based on inconvenient forum or lack of personal jurisdiction.

International Data Transfers. User acknowledges that use of the Service may involve the transfer of data, including Confidential Information and Private Information, to Canada. User consents to such transfers and represents that User has obtained any necessary authorizations or consents required under applicable data protection laws to permit such transfers.

Negotiation. In the event of any dispute arising from or related to this Agreement, the parties shall first attempt to resolve the dispute through good faith negotiation between senior representatives of each party.

Mediation. If the dispute is not resolved through negotiation within thirty (30) days, the parties shall attempt to settle the dispute by mediation administered by a mutually agreed-upon mediator in the Province of Ontario. Each party shall bear its own costs in mediation and shall share equally the fees and expenses of the mediator.

Litigation. If the dispute is not resolved by mediation within sixty (60) days, either party may bring an action in the courts of competent jurisdiction located in Ontario, Canada. The parties consent to the exclusive jurisdiction of these courts and waive any right to trial by jury.

Injunctive Relief. Notwithstanding the above, either party may seek injunctive or other equitable relief to protect its Confidential Information or intellectual property rights in any court of competent jurisdiction without first engaging in negotiation or mediation.

Prevailing Party. In the event of any legal action or proceeding between the parties arising out of this Agreement, the prevailing party shall be entitled to recover reasonable legal fees and costs from the other party.

Language. The parties have expressly requested that this Agreement and all related documents be drafted in English. Les parties ont expressément demandé que cette convention ainsi que tous les documents qui s'y rattachent soient rédigés en anglais.

12. General Provisions

Entire Agreement. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous communications and proposals.

Amendments. Infiltrate may modify this Agreement by providing at least thirty (30) days' notice prior to any material changes taking effect. Such notice may be provided through the Service interface or via email. User's continued use of the Service after such changes become effective constitutes acceptance of the modified Agreement.

Assignment. Neither party may assign this Agreement without the prior written consent of the other party, except that either party may assign this Agreement to an Affiliate or in connection with a merger, acquisition, or sale of all or substantially all of its assets.

Severability. If any provision of this Agreement is found to be illegal, invalid, or unenforceable, such provision shall be enforced to the maximum extent permitted, and the remaining provisions shall continue in full force and effect.

Waiver. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right.

Independent Contractors. The parties are independent contractors. This Agreement does not create a joint venture, partnership, or agency relationship between the parties.

Notices. Any notice required under this Agreement shall be in writing and shall be deemed received: (i) upon personal delivery; (ii) upon confirmation of receipt if sent by email; or (iii) two (2) business days after deposit with a nationally recognized overnight courier. Notices to Infiltrate shall be sent to legal@infiltrateiq.com or by overnight courier to InfiltrateIQ Inc., 77 City Centre Drive, Suite 501, Mississauga, ON L5B 1M5. Notices to User shall be sent to the mailing address and email address associated with User's account; email notice alone is not sufficient for termination, breach, or legal proceedings.

Export Compliance. Each party acknowledges that Confidential Information may include technical data developed in Canada or the United States and shall not export or re-export any Confidential Information without full compliance with all applicable export laws.

Counterparts. This Agreement may be executed in counterparts and delivered via electronic transmission, each of which shall be deemed an original.

13. Fees and Payment

Service Fees. User agrees to pay the fees for the Service as set forth in the applicable order form, pricing page, or statement of work. All fees are quoted and payable in Canadian Dollars (CAD) unless otherwise specified.

Payment Terms. Unless otherwise specified, fees are due within thirty (30) days of invoice date. Late payments shall bear interest at the rate of one and one-half percent (1.5%) per month, or the maximum rate permitted by law, whichever is less.

Taxes. All fees are exclusive of applicable taxes. User is responsible for paying all taxes, including sales, use, GST, HST, PST, VAT, and similar taxes, excluding taxes based on Infiltrate's net income.

Testing Disruption Fees. If a Penetration Test cannot proceed or must be repeatedly restarted due to issues with the Target Environment that are attributable to User (including but not limited to Target Environment instability, unavailability, configuration changes during testing, inadequate resources, or failure to provide required access), the following provisions shall apply:

(i) Infiltrate shall notify User of the issue and provide User with a reasonable opportunity (not less than twenty-four (24) hours) to remedy the condition;

(ii) If the issue persists or recurs after notice, and Infiltrate's personnel have expended time that cannot be productively applied to the Penetration Test, Infiltrate may charge a Testing Disruption Fee at the rate of CAD $150.00 per hour for documented time lost due to Target Environment issues;

(iii) Testing Disruption Fees shall be invoiced separately with reasonable documentation of the time lost and the nature of the Target Environment issues;

(iv) If cumulative Testing Disruption Fees exceed twenty-five percent (25%) of the original Service fee, either party may elect to terminate the engagement, in which case User shall pay for work completed to date plus accrued Testing Disruption Fees, and Infiltrate shall deliver any partial results obtained;

(v) Testing Disruption Fees shall not apply to issues caused by Infiltrate's testing activities, Force Majeure events, or issues with Infiltrate's own systems or tools.

Fee Disputes. User must notify Infiltrate of any fee dispute within thirty (30) days of the invoice date. The parties shall work in good faith to resolve any disputed amounts. Undisputed amounts remain due according to standard payment terms.

Contact Information

For questions about these Terms and Conditions, please contact:

InfiltrateIQ Inc.

Email: support@infiltrateiq.com

Legal: admin@infiltrateiq.com

Privacy: privacy@infiltrateiq.com

Security: spencer.fairbairn@infiltrateiq.com

By clicking "Accept Terms & Conditions" or using the Service, you agree to be bound by these Terms and Conditions.