Terms of Service

INFILTRA

AI-Powered Web Application Penetration Testing

TERMS OF SERVICE

Version 3.0 | June 2026

> *PLEASE READ CAREFULLY. By clicking "Create Account", "Sign Up", "I Agree", or by otherwise accessing or using the Infiltra platform (including on a Free Plan), you agree to be legally bound by these Terms of Service. If you do not agree, do not register or use the Service. If you are registering on behalf of a company or other legal entity, you represent that you have the authority to bind that entity to these Terms.*

1. PARTIES AND DEFINITIONS

1.1 The Parties

These Terms of Service ("Terms") constitute a binding agreement between Infiltra, a trading name of Crysp Australia Pty Ltd (ABN 17 608 341 448) ("Infiltra", "we", "us", or "our"), and the individual or entity registering for or using the Service ("Customer", "you", or "your").

1.2 Definitions

The following terms have specific meanings throughout these Terms:

"Application"	A single web application or API that you register within the Platform for security testing, associated with a defined scope (domain, URL range, or IP range) and one or more environment labels.
"Application Credential"	Any username, password, API key, token, session cookie, or other authentication material that you provide to the Platform to enable authenticated (gray box) Scans.
"Authorized User"	An individual granted access to the Platform by you, whether as an administrator, operator, or viewer.
"Environment"	A distinct deployment instance of an Application, such as production, staging, UAT, or development, identified by a different URL, domain, or IP address.
"Free Plan"	The no-cost access tier made available by Infiltra at its discretion, with entitlements as published on the Pricing Page.
"Plan"	The subscription or access tier selected by you (including the Free Plan), whose current entitlements — including Projects, Applications, and Scans — are described on the Pricing Page.

"Platform / Service"	The cloud-hosted, AI-powered, automated web application and API penetration testing service operated by Infiltra, including all dashboards, reports, APIs, documentation, and supporting infrastructure.
"Pricing Page"	Infiltra's current pricing and plan entitlements page at infiltra.ai/pricing.html, as updated from time to time.
"Project"	A logical grouping within the Platform that may contain one or more Applications.
"Scan"	A single automated penetration-testing or security-assessment execution initiated against an Application through the Platform.
"Scan Data"	All data generated or produced by the Platform as a result of a Scan, including findings, vulnerability reports, evidence, payloads, and logs.
"User Credentials"	The login credentials (username, password, SSO token, MFA code, or similar) used by an Authorized User to access the Platform itself.

1.3 Interpretation

References to "including" are non-exhaustive. The singular includes the plural. Headings are for convenience only.

2. ACCOUNT REGISTRATION AND FREE PLAN

2.1 Eligibility

You must be at least 18 years of age and legally capable of entering binding contracts to register for the Service. By registering, you confirm that all information you provide is accurate, current, and complete.

2.2 Free Plan Access

Infiltra offers a Free Plan that allows you to access and use the Platform at no charge, subject to the entitlements published on the Pricing Page. The Free Plan is provided as a convenience and is subject to these Terms in their entirety. Infiltra reserves the right to modify, suspend, limit, or discontinue the Free Plan at any time, with or without notice, for any reason including security, misuse, operational, or legal reasons.

2.3 One Account Per Entity

Each individual or organization may register only one Free Plan account. Creating multiple Free Plan accounts to circumvent plan limits is a material breach of these Terms and will result in immediate suspension of all associated accounts.

2.4 Upgrades

You may upgrade to a paid Plan at any time. Paid Plans are governed by these Terms together with any additional terms confirmed at checkout or in a separate Order Form. Plan entitlements for all tiers are as

published on the Pricing Page at the time of subscription.

3. LICENSE GRANT AND RESTRICTIONS

3.1 License

Subject to your compliance with these Terms, Infiltra grants you a limited, non-exclusive, non-transferable, revocable right to access and use the Platform during the term of your Plan, solely to perform security testing of Applications that you own or are expressly authorized to test.

3.2 Restrictions

You must not, and must ensure your Authorized Users do not:

- use the Platform to scan any system, application, or asset you do not own or for which you do not hold valid written authorization from the system owner;
- resell, sublicense, or make the Platform available to third parties as a bureau, managed, or white-label service without Infiltra's prior written consent;
- permit any third-party organization to access or use the Platform through your account, whether by sharing credentials, providing API keys, or any other means, without Infiltra's prior written consent;
- reverse engineer, decompile, or attempt to extract the source code, AI models, or algorithms underlying the Platform;
- systematically extract, scrape, or harvest vulnerability intelligence, detection signatures, or testing methodology from the Platform for any purpose;
- use the Platform for any unlawful purpose or in violation of applicable cybercrime, privacy, or computer access laws;
- circumvent or interfere with any access controls, rate limits, or security mechanisms within the Platform;
- introduce malware, exploits, or malicious content into the Platform; or
- use the Platform to cause harm to third-party systems, networks, or data.

4. AUTHORIZATION TO TEST — YOUR REPRESENTATIONS

4.1 Ownership and Authorization Warranty

This is one of the most important obligations in these Terms. Automated penetration testing directed at systems you do not own or are not authorized to test is illegal in most jurisdictions.

By registering any Application and initiating any Scan, you represent and warrant — on each occasion — that:

- you are the legal owner of the Application, or you hold current, valid, written authorization from the legal owner permitting security testing of that Application;
- the authorization covers the specific scope, environments, and testing techniques you intend to use;
- you have the legal right to receive and act upon Scan Data generated from the Application; and

you have obtained any consents required by applicable privacy law in relation to personal data that may be encountered during Scans.

4.2 Your Responsibility for Scope

You are solely responsible for correctly configuring the scope of each Scan, including target domains, URL ranges, IP addresses, authenticated paths, and any excluded areas. Infiltra does not independently verify whether you are authorized to test any Application. Responsibility for any testing activity that exceeds the authorized scope rests entirely with you.

4.3 Third-Party Hosting

Where an Application is hosted on infrastructure operated by a cloud provider, CDN, or hosting company, you are solely responsible for reviewing and complying with that provider's acceptable-use and penetration-testing notification requirements. Infiltra is not liable for any breach of third-party provider terms arising from Scans you direct.

4.4 No Authorization Conferred by Infiltra

Infiltra's grant of a license to use the Platform does not constitute authorization to test any specific system. Your authorization to test must derive entirely from your own ownership or from the written permission of the system owner.

5. PLAN ENTITLEMENTS AND PERMITTED USE

5.1 Entitlements Governed by the Pricing Page

Your Plan determines the number of Projects, Applications, and Scans you may use. Current entitlements for each Plan, including the Free Plan, are published on the Pricing Page at infiltra.ai/pricing.html. Infiltra may update Plan entitlements from time to time in accordance with Section 20. The Pricing Page, not these Terms, is the authoritative reference for current quotas.

5.2 What Your Entitlements Mean

Regardless of the specific limits of your Plan, the following principles govern how entitlements may be used:

Your Plan includes an Application quota and a Scan quota.
The Application quota limits the number of distinct web applications or APIs you may have under active registration.
The Scan quota limits the total number of Scans you may initiate across those applications.
Unused Scans do not roll over to subsequent periods unless expressly stated on the Pricing Page.
A Project is a container for one or more Applications. Project and Application quotas are independent limits; both apply.
Current quotas and their applicable periods are published on the Pricing Page.

5.3 Permitted Flexibility — Environment Rotation

This clause allows you to test the same application across staging and production environments without that counting as two separate applications — while preventing the quota from being used to cycle through unrelated applications.

You may update a registered Application's target URL or domain to reflect a different Environment of the same underlying application. This is permitted provided:

- the Application represents the same underlying software product or service;
- the URL or domain change reflects a genuine environment distinction for that application, not a different application entirely;
- you update the environment label within the Application registration when switching; and
- the flexibility is not used to rotate through a larger pool of unrelated applications than your Plan permits.

5.4 What Constitutes Misuse of Plan Limits

The following practices are prohibited and constitute misuse that may result in suspension or termination:

- registering, scanning, and de-registering unrelated applications on a rotating basis to stay within your Application quota ("application cycling");
- using a single Application registration to test materially different software products, or to scan applications belonging to different organizations;
- creating multiple accounts (including Free Plan accounts) to aggregate entitlements that would otherwise require a higher Plan; and
- artificially splitting a single application across multiple Project or Application registrations to circumvent limits.

5.5 Infiltra's Right to Determine Misuse

Infiltra reserves the right, acting reasonably, to determine whether your use of the Platform constitutes misuse of Plan limits. Where Infiltra makes such a determination, it may suspend access, require a Plan upgrade, or terminate these Terms in accordance with Section 15.

5.6 Usage Monitoring

Infiltra may monitor usage metadata, including Scan frequency, Application registrations, user activity patterns, and quota consumption to verify compliance with Plan entitlements, detect misuse, prevent abuse, and protect the Platform. This monitoring is limited to Platform usage data and does not extend to monitoring your Applications or systems.

6. AUTHORIZED USERS AND ACCESS CONTROL

6.1 Customer's Responsibility for Users

You are solely responsible for:

determining who is granted Authorized User status;
promptly revoking access for individuals who leave your organization, change roles, or no longer require access;
implementing role-based access controls (RBAC) appropriate to each user's function; and
ensuring every Authorized User is aware of and complies with these Terms.

6.2 Liability for User Actions

All acts and omissions of your Authorized Users in connection with the Platform are treated as your own. You are liable for any breach of these Terms by an Authorized User as if you had committed it directly.

6.3 No Credential Sharing

Authorized Users must not share, transfer, or disclose their User Credentials to any other person. Credential sharing is a material breach of these Terms.

6.4 Insider Threat Responsibility

Infiltra is not responsible for the actions of any current, former, or departing Authorized User who uses knowledge, findings, or information obtained through the Platform to cause harm to any system, whether during or after their period of authorized access. You are solely responsible for managing insider threat risks associated with your use of the Platform, including implementing appropriate access controls, monitoring user activity within the Platform, and ensuring adequate offboarding procedures for departing personnel. This applies regardless of whether the individual was acting within or outside the scope of their authorized role at the time of the harmful act.

7. CREDENTIAL SECURITY AND BREACH RESPONSE

7.1 User Credentials

You are solely responsible for maintaining the confidentiality and security of all User Credentials. If you become aware or have reasonable grounds to suspect that any User Credentials have been compromised, regardless of how or where the compromise occurred, you must:

immediately change the affected User Credentials within the Platform;
revoke all active sessions associated with the compromised account;
notify Infiltra at security@infiltra.ai within 24 hours of discovery; and
review recent Platform activity for any unauthorized Scans or data access.

7.2 Application Credentials

Where you provide Application Credentials to enable authenticated Scans, you agree to:

use dedicated, purpose-limited service accounts or API tokens with the minimum privilege necessary for the Scan, not shared or administrator credentials;
immediately revoke and replace any Application Credentials that you suspect have been compromised, and update the affected Application registration in the Platform without delay —

regardless of whether the compromise occurred through or outside of the Platform;
notify Infiltra at security@infiltra.ai within 24 hours if you determine that Application Credentials stored in the Platform have been accessed by an unauthorized party; and
rotate Application Credentials regularly and in any event upon any security incident affecting your organization.

7.3 No Liability for External Compromise

Infiltra is not responsible for loss or harm arising from the compromise of User Credentials or Application Credentials where the compromise originates from events or systems outside the Infiltra Platform, including phishing, malware, third-party data breaches, or your internal security incidents. The obligation to respond immediately rests with you regardless of the source of compromise.

7.4 Infiltra's Handling of Credentials

Infiltra encrypts Application Credentials at rest and in transit using industry-standard methods. Credentials are used solely to execute Scans as configured by you and are not accessed by Infiltra personnel except where required to diagnose a technical issue at your request.

8. ACCEPTABLE USE POLICY

8.1 Permitted Use

The Platform is licensed exclusively for lawful, authorized security testing of web applications and APIs for the purpose of identifying and remediating security vulnerabilities.

8.2 Prohibited Conduct

You must not use the Platform to:

scan, probe, or attack any system for which you lack legal authority;
conduct Denial of Service attacks or testing designed to cause sustained unavailability beyond the inherent and reasonable effects of penetration testing;
retain, exploit, or exfiltrate real sensitive data, including personal data, payment card data, or credentials encountered incidentally during a Scan;
use Scan Data, vulnerability findings, or reports to cause deliberate damage to any system, exfiltrate data, deploy malware, or facilitate unauthorized access by any third party;
use Scan Data or reports to threaten, coerce, extort, or exert improper pressure on any person or organization;
misrepresent Scan results or reports as a formal certification or audit opinion issued by an accredited body, noting that use of reports as evidence of penetration testing within a broader compliance program is permitted and encouraged;
conduct testing in a manner that causes material collateral impact to systems shared with parties other than you;
interfere with or disrupt the Platform or Infiltra's infrastructure;
facilitate extortion, ransomware, fraud, or any criminal activity; or

export the Platform or Scan results in violation of applicable export control laws.

8.3 Responsible Disclosure

If you discover a security vulnerability in the Infiltra Platform itself, you agree to notify Infiltra promptly at security@infiltra.ai and not to publicly disclose the vulnerability without first allowing Infiltra a minimum of 90 days to investigate and remediate. Any disclosure must not include customer data, exploit code, Application Credentials, platform secrets, or information that could materially increase risk to Infiltra or its customers.

8.4 Scan Throttling and Operational Control

Infiltra may throttle, pause, cancel, or refuse Scans where it reasonably believes the Scan may cause harm, breach applicable law, exceed the authorized scope, trigger third-party complaints, or affect Platform stability. Infiltra will use reasonable efforts to notify you where a Scan is interrupted, but is not liable for any loss arising from the interruption.

9. NATURE OF PENETRATION TESTING — DISRUPTION ACKNOWLEDGMENT

9.1 Inherent Effects of Scanning

You acknowledge that automated penetration testing is inherently intrusive and may, by its nature, cause:

- temporary performance degradation or reduced responsiveness of target Applications and associated infrastructure;
- alerts, events, and notifications within your security monitoring, WAF, SIEM, or IDS/IPS systems;
- test artifacts, log entries, or records within Application databases or storage; and
- disruption to non-critical application functions during fault-injection or authentication-bypass testing.

You accept these consequences as inherent to the nature of penetration testing and agree that Infiltra is not liable for any such effects.

9.2 Your Pre-Scan Obligations

Before initiating any Scan, you should, where appropriate:

- notify relevant internal teams (operations, DevOps, security, compliance) of the planned Scan;
- obtain approval from the system owner and any relevant third-party hosting provider;
- configure the scope to exclude systems or paths not intended for testing;
- ensure monitoring and rollback procedures are in place; and
- follow your organization's change management process.

9.3 Production Environment Risk

Infiltra recommends against running high-intensity Scans against production environments without appropriate safeguards. You are solely responsible for the resilience, backup, and recoverability of Applications and their data before initiating Scans. Infiltra is not liable for any degradation, data loss, or incidents occurring in your environments as a result of Scans you initiate.

9.4 Your Security Environment

Infiltra is not responsible for securing, monitoring, backing up, patching, configuring, or remediating your Applications, infrastructure, identity systems, source code, cloud environments, third-party services, or operational processes. Your use of the Platform does not transfer or delegate any aspect of your security responsibilities to Infiltra.

10. SCAN DATA, PRIVACY, AND DATA HANDLING

10.1 Your Ownership of Scan Data

You retain all right, title, and interest in Scan Data generated from your Applications. Infiltra does not claim ownership of your Scan Data.

10.2 Infiltra's Limited Use of Scan Data

Infiltra may use your Scan Data only to provide and maintain the Service to you. Infiltra will not sell, rent, or disclose your identifiable Scan Data to third parties except as required by law or with your prior written consent.

10.3 Data Retention

Scan Data is retained for the period specified on the Pricing Page or in your Plan documentation. Upon expiry or termination of your account (other than for cause), you may export your Scan Data for 30 days. Infiltra will securely delete all Customer data within 30 days of the end of that access period, unless retention is required by law. You are responsible for exporting Scan Data you wish to retain beyond the applicable retention period. Infiltra is not liable for loss of Scan Data deleted after the retention period.

10.4 Customer-Modified Findings

Where the Platform allows you to annotate, update, or change the status of findings within Scan Data or reports, you are solely responsible for the accuracy of any such modifications. Infiltra's reports reflect the state of findings at the time of the Scan. Any subsequent changes made by you, including marking findings as resolved, adjusting severity, or adding commentary, are your representations, not Infiltra's. Infiltra accepts no responsibility for the accuracy of modified reports or for any third party's reliance on them.

10.5 Report Distribution

You are responsible for controlling the distribution of reports and Scan Data and for any consequences of sharing them with auditors, regulators, customers, insurers, investors, or other third parties. Once a report leaves the Platform, Infiltra has no control over its use or further distribution and accepts no liability for claims arising from third-party access to reports you have shared.

10.6 Personal Data Encountered During Scans

You are the data controller for any personal data your Scans encounter. Infiltra acts as a data processor in respect of that data. You are responsible for ensuring you have a lawful basis for any personal data processed during Scans.

10.7 Privacy Policy

Infiltra's collection and use of personal data relating to Authorized Users is governed by the Privacy Policy at infiltra.ai web site, incorporated into these Terms by reference.

11. FEES AND PAYMENT

11.1 Fees

Fees for paid Plans are as specified on the Pricing Page at the time of subscription or as agreed in a separate Order Form. All fees are in US Dollars (USD) unless otherwise stated and are non-refundable except as required by law.

11.2 Billing and Payment

Fees for paid Plans are charged automatically via the payment method you provide at the time of subscription. Payment is processed immediately at the start of each billing cycle. If a payment fails, Infiltra may reattempt the charge. If payment remains unsuccessful for more than 10 business days, Infiltra may suspend access to the Platform until payment is received. You are responsible for ensuring your payment method remains valid and current.

11.3 Auto-Renewal

Paid Plans renew automatically at the end of each billing period at the then-current price unless you cancel before the renewal date through the Platform's account settings.

11.4 Price Changes

Fees for paid Plans are as published on the Pricing Page. Infiltra may update pricing at any time. The price in effect on the Pricing Page at the time of your renewal applies to your next billing cycle.

11.5 Taxes

All fees are exclusive of GST, VAT, and other applicable taxes. You are responsible for paying all applicable taxes in addition to the fees. Infiltra will issue valid tax invoices where required.

11.6 No Set-Off

You may not withhold or set off any amount owed to Infiltra against any claim or amount you believe Infiltra owes to you unless agreed in writing or required by law.

12. LIMITATION OF LIABILITY

12.1 Exclusion of Consequential Loss

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING LOSS OF PROFITS, REVENUE, BUSINESS OPPORTUNITY, GOODWILL, OR DATA, ARISING OUT OF OR IN CONNECTION WITH THESE TERMS, REGARDLESS OF HOW THE CLAIM ARISES AND EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12.2 Aggregate Liability Cap

TO THE MAXIMUM EXTENT PERMITTED BY LAW, INFILTRA'S TOTAL AGGREGATE LIABILITY TO YOU FOR ALL CLAIMS UNDER OR RELATING TO THESE TERMS — INCLUDING UNDER ANY INDEMNITY — SHALL NOT EXCEED THE TOTAL FEES PAID BY YOU TO INFILTRA IN THE TWELVE (12) MONTHS PRECEDING THE CLAIM.

12.3 Free Plan Liability

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, INFILTRA EXCLUDES ALL LIABILITY IN CONNECTION WITH THE FREE PLAN. THE FREE PLAN IS PROVIDED PURELY AS A COURTESY WITH NO WARRANTIES OF ANY KIND.

12.4 Exceptions

Nothing in these Terms limits either party's liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, or any other liability that cannot be lawfully excluded under the Australian Consumer Law or other applicable mandatory law.

12.5 Allocation of Risk

The liability limitations in this Section reflect a reasonable allocation of risk between the Parties. Infiltra would not offer the Service — including the Free Plan — without these limitations.

13. DISCLAIMER OF WARRANTIES

13.1 As-Is Service

THE PLATFORM IS PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, INFILTRA DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

13.2 No Guarantee of Complete Coverage

You acknowledge that:

- the Platform is an automated tool and may not detect all vulnerabilities or misconfigurations in an Application;
- Scan results reflect the state of the Application at the time of the Scan and do not account for changes made before or after;
- a clean Scan result does not mean the Application is secure; and
- Infiltra makes no guarantee as to Scan coverage depth, technique breadth, or finding accuracy.

13.3 Not a Certification Body

Infiltra is a penetration testing platform, not an accredited certification body. Scan results and reports are penetration test outputs that may be used as evidence of security testing within your compliance programs. They do not constitute, and must not be represented as, a formal certification or audit opinion issued by an accredited body. You are solely responsible for your own regulatory and compliance obligations.

13.4 AI-Generated Outputs

The Platform uses artificial intelligence to generate findings, severity ratings, remediation guidance, exploit narratives, and recommendations. AI-generated outputs may be incomplete or inaccurate and must be reviewed and validated by suitably qualified personnel before being relied upon or acted upon.

13.5 False Positives and False Negatives

Automated scanning may produce false positives (findings for vulnerabilities that do not exist) or false negatives (missing vulnerabilities that do exist). You are responsible for validating findings before acting on them.

13.6 Beta and Experimental Features

Infiltra may from time to time make beta, preview, or experimental features available within the Platform. These features may be incomplete, unstable, or changed or withdrawn without notice. You use beta features at your own risk and they are provided without any warranty whatsoever.

13.7 No Professional Advisory Service

The Platform does not provide legal, compliance, audit, risk management, or professional security consulting advice. If you require such services, you must engage appropriately qualified professionals separately.

14. INDEMNIFICATION

14.1 Your Indemnity to Infiltra

You will defend, indemnify, and hold Infiltra and its personnel harmless from any claim, loss, liability, damage, or expense (including reasonable legal fees) arising from:

- your breach of the authorization warranty in Section 4.1;
- any Scan conducted against a system you were not authorized to test;
- your violation of any law, regulation, or third-party right;
- any act or omission of your Authorized Users, including acts by current, former, or departing Authorized Users using knowledge or information obtained through the Platform;
- any third-party claim arising from reliance on reports, findings, or Scan Data that you have modified, annotated, or exported from the Platform, including where findings have been marked as resolved without actual remediation; or
- damage caused to third-party systems or data as a result of Scans you direct.

14.2 Infiltra's Indemnity to You

Infiltra will defend you against any third-party claim that the Platform (excluding your content, Applications, and any third-party or open-source components) infringes a third party's intellectual property rights, provided you promptly notify Infiltra of the claim and grant Infiltra reasonable control of the defense. Infiltra's indemnity does not apply where the alleged infringement arises from your content, your instructions, modifications you have made, combination of the Platform with other products or services, or use of the Platform outside the scope of these Terms. This indemnity is subject to the limitations and exclusions in Section 12.

15. SUSPENSION AND TERMINATION

15.1 Termination by You

You may stop using the Service and close your account at any time. For paid Plans, you may terminate at the end of the current billing period in accordance with the cancellation process on the Platform. Fees paid are non-refundable unless required by law.

15.2 Suspension or Termination by Infiltra

Infiltra may immediately suspend your access to the Platform or terminate these Terms if:

- you breach the authorization warranty in Section 4.1;
- Infiltra reasonably determines you are engaged in misuse of Plan entitlements as described in Section 5.4;
- you violate the Acceptable Use Policy in Section 8;
- Infiltra determines, acting reasonably, that your use of the Platform is fraudulent, deceptive, or intended to cause harm to third parties;
- you fail to pay applicable Fees and do not remedy the failure within 10 business days of notice;
- you are subject to insolvency proceedings or winding-up;
- Infiltra is required to do so by law, court order, or regulatory direction; or
- Infiltra reasonably determines that continued provision of the Service poses a material legal, regulatory, or reputational risk.

15.3 Suspension as a Precaution

Infiltra may suspend access without terminating these Terms where a breach is remediable, providing you a reasonable opportunity to cure. Suspension does not waive Infiltra's right to subsequently terminate.

15.4 Discontinuation of Access for Misuse

Infiltra retains the right to discontinue access or service to any Customer where Infiltra has reasonable grounds to believe the Platform is being used inconsistently with these Terms. Where commercially practicable, Infiltra will provide notice before doing so.

15.5 Effect of Termination

Upon termination or expiry:

- your license to use the Platform ceases immediately;
- you must cease all use of the Platform and destroy or return any Infiltra materials;
- for terminations not for cause, you may export Scan Data for 30 days following termination;
- for terminations for cause, including fraud, unauthorized scanning, or Acceptable Use Policy violations, access may be revoked immediately without a data export window; and
- all accrued payment obligations survive termination.

16. INTELLECTUAL PROPERTY

16.1 Infiltra's IP

All right, title, and interest in the Platform, including its software, AI models, autonomous agents, algorithms, scanning methodology, vulnerability intelligence, user interface, documentation, and trademarks are and remain the exclusive property of Infiltra. These Terms do not transfer any ownership rights to you.

16.2 Feedback

If you provide suggestions, feature requests, or other feedback about the Platform, you grant Infiltra a perpetual, irrevocable, royalty-free license to use and incorporate that feedback without obligation to you.

16.3 Your Content

You retain all rights in your Applications, Application Credentials, and Scan Data. You grant Infiltra only the limited license necessary to operate the Platform and deliver the Service as described in Section 10.2.

17. CONFIDENTIALITY

17.1 Mutual Obligations

Each Party agrees to keep confidential all non-public information of the other that is designated confidential or that reasonably ought to be treated as confidential. Infiltra's confidential information includes its Platform architecture, AI models, scanning methodology, and pricing. Your confidential information includes Scan Data, User Credentials, Application Credentials, and Application details.

17.2 Exceptions

Confidentiality obligations do not apply to information that: (a) becomes publicly known through no fault of the receiving Party; (b) was already known to the receiving Party; (c) is independently developed without reference to the confidential information; or (d) must be disclosed by law or court order, with reasonable advance notice given.

17.3 Publicity and Logos

Neither party may use the other's name, logo, or trademarks in any press release, public announcement, or marketing material without the other party's prior written consent.

17.4 Survival

Confidentiality obligations survive termination for three (3) years.

18. LEGAL COMPLIANCE AND EXPORT CONTROLS

18.1 Your Compliance Obligations

You are solely responsible for ensuring your use of the Platform complies with all applicable laws in each jurisdiction where you operate or where Applications are hosted, including cybercrime legislation, privacy law, and any sector-specific security requirements.

18.2 Export Controls

The Platform may be subject to Australian, US, and EU export control regulations. You agree not to export or transfer access to the Platform in violation of applicable export laws, and represent that you are not on any applicable denied party list.

18.3 Regulatory Reporting

Where applicable law requires you to notify regulators or individuals of vulnerabilities discovered through Scans, you are solely responsible for making those notifications. Infiltra bears no responsibility for your regulatory reporting obligations.

19. SERVICE AVAILABILITY

19.1 No Uptime Guarantee (Free and Starter Plans)

For Free Plan and Starter Plan customers, Infiltra does not guarantee any specific level of Platform availability and provides the Service on a commercially reasonable-efforts basis. Uptime commitments and SLAs are available only where expressly specified in a paid Plan or separate agreement.

19.2 Maintenance

Infiltra may take the Platform offline for scheduled maintenance. Infiltra will use reasonable endeavors to provide advance notice and to schedule maintenance during off-peak hours.

19.3 No Liability for Downtime

Infiltra is not liable for Scan failures, data loss, or business impact resulting from Platform unavailability, whether scheduled or unscheduled.

20. CHANGES TO THESE TERMS AND PRICING

20.1 Changes to these Terms

Infiltra may update these Terms from time to time. Where changes are material, Infiltra will provide reasonable notice by email or in-Platform notification. Your continued use of the Platform after the effective date constitutes acceptance. If you do not accept a change, you may close your account before it takes effect.

20.2 Changes to Plan Entitlements

Plan entitlements, including the number of Projects, Applications, and Scans are published on the Pricing Page and may be updated by Infiltra. Changes to paid Plan entitlements for existing subscribers will be communicated with reasonable notice before taking effect.

20.3 No Amendment by Reference

The Pricing Page governs what you are entitled to use; it does not form part of these Terms for the purposes of defining prohibited conduct, liability, or dispute resolution. These Terms control those matters and cannot be varied by Pricing Page updates.

21. GOVERNING LAW AND DISPUTES

21.1 Governing Law

These Terms are governed by the laws of Victoria, Australia, without regard to conflict of law principles.

21.2 Dispute Resolution

The Parties will attempt to resolve disputes through good-faith negotiation. If unresolved within 30 days of written notice, either Party may refer the dispute to non-binding mediation administered by the Australian Disputes Centre before commencing court proceedings.

21.3 Jurisdiction

Subject to the foregoing, each Party submits to the exclusive jurisdiction of the courts of Victoria, Australia.

21.4 Consumer Law

Nothing in these Terms excludes rights that cannot be excluded under the Australian Consumer Law or other applicable mandatory law, including non-excludable consumer guarantees in respect of services.

22. GENERAL

22.1 Entire Agreement

These Terms, together with the Privacy Policy and any incorporated addenda, constitute the entire agreement between the Parties on the subject matter and supersede all prior representations and understandings.

22.2 Order of Precedence

In the event of conflict: (1) any signed Enterprise Order Form or Addendum prevails; (2) these Terms; (3) other referenced policies.

22.3 Severability

If any provision is found invalid or unenforceable, it will be modified to the minimum extent necessary, and the remainder continues in full force.

22.4 Waiver

Failure to enforce any provision does not constitute a waiver of that provision or any other right.

22.5 Assignment

You may not assign these Terms without Infiltra's prior written consent. Infiltra may assign these Terms in connection with a merger, acquisition, or sale of its business with written notice to you.

22.6 Force Majeure

Neither Party is in breach for failures caused by circumstances beyond reasonable control, including natural disasters, war, pandemic, cyberattacks on national infrastructure, or failure of third-party internet, hosting, or cloud services.

22.7 Notices

Notices to Infiltra must be sent to legal@infiltra.ai. Notices to you will be sent to the email address on your account. Notices are effective on confirmed delivery.

22.8 Independent Contractors

The Parties are independent contractors. Nothing in these Terms creates a partnership, joint venture, employment, or agency relationship.

22.9 Survival

Sections 4 (Authorization), 10 (Data), 11 (Fees), 12 (Limitation of Liability), 13 (Disclaimers), 14 (Indemnification), 16 (IP), 17 (Confidentiality), 21 (Governing Law), and 22 (General) survive expiry or termination of these Terms.

ACCEPTANCE

By clicking "Create Account", "Sign Up", or "I Agree" — or by otherwise accessing or using the Platform — you confirm you have read, understood, and agree to be legally bound by these Terms of Service. If registering on behalf of an organization, you confirm you have authority to bind that organization.
