Off Grid Software Terms of Service

LAST UPDATED **August 2, 2026** SECTIONS **111**
PUBLISHED AT **cink.in**

This is the complete document. The version published at cink.in is the same text, built from the same source, and is the version in force. Section numbering, headings and wording match the web copy exactly.

1. Parties and Acceptance

These Terms of Service are between:

- Provider: Deliri Software Inc., operating as Off Grid Software, with offices at 40 Frank Faubert Drive, Scarborough, Ontario, M1C 5H7, Canada ("Off Grid Software", "Provider", "we", "us", or "our").
- Client: the person, company, organization, or other legal entity that accesses, purchases, subscribes to, downloads, installs, or uses the Services or Products ("Client", "Customer", "you", or "your").

If you access, purchase, subscribe to, download, install, or use the Services or Products on behalf of a company, organization, or other legal entity, you represent that you have authority to bind that entity to these Terms. In that case, "Client", "Customer", "you", and "your" refer to that entity. If you do not have that authority, you must not accept these Terms or use the Services or Products on behalf of that entity.

Provider and Client may each be called a "Party" and together the "Parties".

Off Grid Software is a brand, trade name, product name, or public-facing business name of Deliri Software Inc. Unless a signed Order expressly states otherwise, Deliri Software Inc. is the legal contracting entity, owner of Provider rights, payee of Provider

invoices, and party entitled to enforce this Agreement. Use of a brand, product name, website name, statement descriptor, support name, email domain, invoice memo, legacy name, or marketing name does not create a separate contracting party and does not change the Parties' rights or obligations.

These Terms apply to all access to and use of the Off Grid Properties and to Provider websites, downloadable binaries, software products, hosted services, statements of work, proposals, order forms, product subscriptions, license keys, invoices, support plans, hosting plans, maintenance plans, renewals, and change orders accepted by Client, unless a later written agreement signed by Provider expressly states that it overrides these Terms.

2. Business-to-Business Use Only

The Services and Products are offered only for business, professional, internal operational, software development, audit preparation, and commercial use. They are not offered to consumers for personal, family, or household use. Client represents that it is entering into these Terms for business purposes and has authority to bind the business or organization on whose behalf it uses the Services or Products.

Any individual who accepts these Terms, creates an account, or uses the Services or Products on behalf of Client must be at least eighteen years old or the age of majority in that individual's jurisdiction, whichever is higher.

Client represents that it is not buying or using the Services or Products as a consumer under Quebec, Ontario, Canadian, U.S., or other consumer-protection law. If Client is located in Quebec or serves Quebec users, Section 2B states the additional terms that apply, and Client remains responsible for the Quebec laws that apply to Client's own business, customers, employees, language obligations, consumer relationships, privacy obligations, tax obligations, marketing, and use of the Services or Products.

To the maximum extent permitted by law, Client agrees that these Terms are governed by Ontario law, disputes must be handled in Ontario under these Terms, and Client will not bring claims against Provider in Quebec or any other province, state, or country outside the Ontario forum stated in these Terms. Any mandatory non-waivable law applies only to the minimum extent required and

does not change the Parties' chosen law, forum, arbitration agreement, liability limits, payment obligations, or other terms to the extent those terms can still be enforced.

Before purchasing, subscribing to, or activating a Product, and when creating an account, Client must confirm that it is acquiring and using the Services and Products for business or professional purposes and not as a consumer, and must provide the name of the business or organization on whose behalf it is acting. Provider relies on that confirmation. Provider does not knowingly sell to consumers and may refuse, cancel, suspend, or refund any purchase, account, or subscription that Provider reasonably determines is being acquired or used for personal, family, or household purposes.

2A. Access to and Use of the Off Grid Properties

These Terms govern all access to and use of the Off Grid Properties, whether by a visitor, prospective customer, Client, authorized user, account holder, developer, or agent, and whether or not that person purchases, subscribes to, or pays for anything. By accessing, browsing, creating an account on, signing in to, calling an API of, downloading from, or otherwise using any Off Grid Property, you accept these Terms.

The Off Grid Properties, including the marketing website, marketing sites, landing pages, product and pricing pages, documentation, the web application, account and administrative dashboards, sign-in and sign-up flows, and the public and licensing APIs, are offered for business, professional, and evaluation use and are provided on an "as is" and "as available" basis as described in Section 37. Provider may add, change, limit, suspend, deprecate, or discontinue any Off Grid Property, feature, page, endpoint, or API as described in Section 35B.

Access to and use of the Off Grid Properties is subject to the acceptable use, abuse monitoring, and emergency suspension rules in Section 30A. You must not probe, scan, scrape, overload, disrupt, reverse engineer, or attempt unauthorized access to any Off Grid Property, and you are responsible for all activity under any account, credential, API key, or token issued to you, as described in Sections 7, 30, and 30A. The licensing terms in Section 7A, the product-specific terms for bug, witness, and

peachfuzz in Sections 8, 9, and 9A, and the marketing and performance-claim limits in Section 5A, apply to the corresponding Off Grid Properties.

2B. Quebec Clients, Ontario Law, and Language

Provider is an Ontario company with no establishment in Quebec. Provider serves business clients established in Quebec on the same terms as every other business client, and this section states what a Quebec-established Client agrees to when it accepts these Terms or signs an Order.

A Client that is established, resident, headquartered, or contracting through an establishment in Quebec expressly agrees, having had the opportunity to obtain independent legal advice before accepting:

- That it is contracting with an Ontario business that performs from Ontario, and that the place of contracting, performance, invoicing, and payment is Ontario.
- That this Agreement and every Order are governed by the laws of Ontario and the federal laws of Canada applicable in Ontario, as stated in Section 56, and that no law of Quebec applies merely because Client is located there, uses the Services or Products there, or serves its own customers there.
- That disputes are resolved as stated in Section 54, with the seat of arbitration in Toronto, Ontario, and that any court proceeding permitted by that section belongs to the courts of Toronto, Ontario, as stated in Section 56.
- That it will not start, continue, join, or support a proceeding against Provider before a Quebec court, tribunal, or administrative body, and it waives any objection that the Ontario forum is inconvenient. Article 3148 of the Civil Code of Québec permits parties to a commercial contract to submit their disputes to an authority outside Quebec, and the Parties do so here.
- That it is acquiring and using the Services and Products for business or professional purposes, that it is not a consumer within the meaning of the Consumer Protection Act (Quebec) or Article 3149 of the Civil Code of Québec, and that Section 2 of these Terms applies to it in full.

Provider operates in English only, and says so before anyone buys anything. Provider is a one-person business that does not speak French, does not produce French versions of its contracts, documentation, product interfaces, invoices, notices, or support, and does not undertake to obtain a translation. The Services, Products, Off Grid Properties, this Agreement, each Order, and all related notices, invoices, and communications are provided in English only, and every Client accepts them on that basis.

The Parties have expressly requested that this Agreement and all documents relating to it be drawn up in English. Les parties ont expressément demandé que cette convention et tous les documents qui s'y rattachent soient rédigés en anglais.

A Client that requires a French-language contract, French-language documentation, or French-language dealings should not accept these Terms and should not place an Order, because Provider cannot supply them. Provider will decline any transaction that requires them. This is stated plainly and in advance so that no Client discovers it later.

Client remains responsible under Sections 34A and 53 for the Quebec laws that apply to Client's own business, customers, users, employees, language obligations, consumer relationships, privacy obligations, tax obligations, and marketing. Nothing in this section makes Provider responsible for Client's own Quebec obligations.

Nothing in this section waives a law that cannot be waived. If a mandatory Quebec law, forum, or protection is found to apply despite this section, it applies only to the minimum extent required, and every other provision of this Agreement, including the Ontario governing law and forum in Section 56, continues to apply to the maximum extent permitted.

3. Definitions

"Agreement" means these Terms of Service and all attached or incorporated schedules, statements of work, order forms, invoices, product terms, and change orders.

"Deliverables" means websites, applications, APIs, documentation, configuration, code, designs, reports, test artifacts, evidence packages, integrations, product outputs, or other materials that Provider agrees to deliver under an Order.

"Order" means a signed statement of work, accepted proposal, signed quote, online checkout, license purchase, invoice, subscription order, change order, or other written commercial order accepted by Provider.

"Initial Trial" means the one-time initial trial of an eligible Product subscription described in Section 19A.

"Products" means Provider's proprietary software products, including bug, witness, peachfuzz, related CLIs, agents, daemons, hosted services, APIs, documentation, templates, workflows, and other commercial software made available by Provider.

"Registered Device" means a specific computer, virtual machine, container instance, or other device that Client has activated for a Product under Client's account and to which Provider has issued a Product Lease naming that device.

"Organization License" means a license assigned to Client's organization, permitting Client's authorized users to use the Product on Registered Devices without a per-user, per-repository, per-project, per-core, or per-device price multiplier, subject only to a cap expressly stated in the Order or the published plan.

"Registration Token" means the secret account credential Client obtains from Provider's authenticated website and supplies to a Product's register command to activate a Registered Device. It authenticates registration and is not itself a Product Lease.

"Product Lease" means Provider's signed, device-bound licensing decision described in Section 7A. A Product Lease controls whether a Registered Device may create new licensed work. It is separate from a Retention Lease and does not by itself promise storage or custody.

"Custody Artifact" means the exact, versioned Product evidence that a custody-eligible plan permits Client to submit under Section 7B and the applicable Product terms. A Custody Artifact is separate from a license check-in and does not include source code, secrets, credentials, or any category that the applicable Product terms exclude.

"Retention Lease" means the storage and custody arrangement described in Section 21B. A Retention Lease controls how long Provider holds accepted Custody Artifacts. It does not grant Product use and does not extend a Product Lease.

"Provider Time" means the signed absolute time observation Provider's control plane places in every application-level response to an installed Product. Provider Time is encoded under the versioned temporal contract used by that Product and is not a free-form date string or an unsigned HTTP header.

"Product Status" means the closed status Provider's control plane assigns to an installed Product. The admitted statuses are Active, Payment Retry, Read Only, Stopped, Upgrade Required, and Revoked. There is no Unknown status. A status not admitted by the Product and wire revision is invalid and conveys no authority.

"Usage Window" means one bounded, non-overlapping interval of typed Product usage measurements identified by its start, end, and watermark. A Usage Window is operational telemetry, not a Custody Artifact and not proof that custody occurred.

"Seal" means the operation by which a Product closes a record on the Registered Device that produced it, binding the record's contents with hashes, manifests, and the device signature so that any later alteration causes verification to fail. A record is sealed before it leaves the Registered Device. Sealing is performed by the Product on Client's machine, and Provider does not seal, re-seal, or alter a sealed record.

"Timestamp Authority" means an independent third-party time-stamping authority that issues RFC 3161 timestamp tokens. Provider may relay a Product's timestamp request to a Timestamp Authority and return the resulting token. Provider cannot alter a token so relayed: each token is signed by the issuing authority and is verifiable against that authority's own trust root without Provider's participation.

"Verification Page" means a Provider-operated path by which a person Client chooses can check one specific record that Client identifies, without holding an account with Provider. Access is by a capability link that Client generates and controls, and the path discloses only the record that link names. A Verification Page is not a public listing, directory, index, or search surface, and Provider does not publish Client's identity, records, findings, or account statistics on it.

"Corpus Entry" means one input to a fuzz target that a fuzzing engine retains because it reached program behaviour not previously reached. A Corpus Entry is a byte string. It is

predominantly produced by the engine's mutation of earlier inputs, and it is derived from the seed inputs Client supplies in Client's own repository.

"Cloud Evidence" means the optional peachfuzz feature described in Section 9A.1 by which a Registered Device uploads Corpus Entries and retained finding inputs to tenant-private storage, and other Registered Devices of the same Client retrieve them. Cloud Evidence is off until Client enables it, is available only on plans whose published terms include it, and is separate from a license check-in and from a Custody Artifact.

"Off Grid Properties" means Provider's own public and operated web properties and interfaces, including the Off Grid Software marketing website, marketing sites, landing pages, product and pricing pages, documentation pages, the web application, account and administrative dashboards, sign-in and sign-up flows, the public and licensing APIs, and the downloadable bug, witness, and peachfuzz products, together with the related pages, endpoints, and services operated by Provider.

"Services" means professional services provided by Provider, including website development, application development, API development, consulting, implementation, testing, support, maintenance, hosting management, compliance evidence implementation, product onboarding, and training.

"Client Materials" means content, data, source code, repositories, test suites, configuration, credentials, policies, procedures, designs, trademarks, business rules, records, regulated data, and other materials provided or controlled by Client.

"Provider Background IP" means all technology, software, source code, object code, scripts, libraries, frameworks, templates, processes, know-how, methodologies, products, product roadmaps, designs, tools, agents, testing systems, compliance evidence systems, bug, witness, peachfuzz, general-purpose components, and reusable work product owned, developed, licensed, or used by Provider before, during, or after an Order, excluding Client Materials and Client-owned custom Deliverables expressly assigned under this Agreement.

"Confidential Information" means non-public business, technical, security, financial, legal, customer, source code, product, pricing, credential, audit, compliance, roadmap, or operational information

disclosed by one Party to the other, whether orally, visually, electronically, or in writing.

"Regulated Data" means personal information, personal data, protected health information, payment card data, financial records, government controlled information, export-controlled information, credentials, secrets, or any other data subject to special legal, regulatory, contractual, or industry restrictions.

4. Order of Precedence

If documents conflict, the following order controls:

1. A signed amendment that expressly names the clause it overrides.
2. A signed Order or statement of work.
3. Product-specific terms in this Agreement.
4. This Agreement.
5. Documentation, proposals, website copy, marketing materials, ticket comments, emails, and informal messages.

No marketing page, sales discussion, roadmap statement, demo, estimate, or informal communication creates a warranty, guarantee, service level, legal commitment, certification promise, or acceptance obligation unless it is expressly included in a signed Order.

5. Scope of Services

Provider may provide Services including the following website services:

- Website redesigns.
- Custom websites.
- Landing pages.
- Custom ecommerce stores.
- Web applications.
- API and integrations.

Provider may also provide related Services including:

- Internal tools and operational software.

- API design, development, integration, testing, documentation, and cloud deployment support.
- Checkout, lead capture, booking, CRM, analytics, payment, email, automation, and third-party platform integrations.
- Hosting setup, domain support, SSL/TLS setup, monitoring, support, maintenance, and managed deployment.
- Product implementation, configuration, onboarding, and training for bug, witness, and peachfuzz.
- Testing systems, evidence generation systems, and audit-readiness implementation.
- Code quality, compiler-driven workflow, agent-readable workflow, and software engineering consulting.

Provider is responsible only for the scope expressly stated in the applicable Order. Anything not expressly included is out of scope.

The Parties acknowledge that Client may describe a business symptom rather than a technical specification. Provider may help diagnose whether the appropriate route is a redesign, website, landing page, ecommerce store, web application, API/integration, Product implementation, or another scoped solution. Diagnosis discussions do not expand scope unless captured in an Order.

5A. Marketing and Performance Claims

Provider's website, proposals, demos, case studies, and sales materials may describe positioning, speed, scale, trust, lead generation, conversion, checkout, reliability, quality, or performance goals. Those statements are commercial descriptions and examples only.

No claim about requests per second, zero errors, uptime, latency, scalability, conversion, checkout performance, search ranking, revenue, security, audit readiness, or business impact is a warranty, guarantee, acceptance criterion, service level, or legal commitment unless the applicable Order states the exact metric, test method, test environment, data set, duration, exclusions, and remedy.

Performance depends on many factors outside Provider's control, including Client Materials, hosting environment, traffic mix, third-party APIs, databases, caches, browsers, devices, payment processors, DNS, networks, integrations, and Client operations.

6. No Informal Scope Expansion

Scope may not be expanded by Slack messages, emails, calls, comments in tickets, pull request comments, verbal statements, screenshots, demos, or assumptions. Out-of-scope work requires a written change order or written approval by Provider stating the scope, fee, and timeline impact.

Provider may choose to perform small out-of-scope items without waiving its right to charge for future out-of-scope work.

7. Client Responsibilities

Client will:

- Provide timely access to systems, repositories, domains, accounts, environments, documentation, personnel, policies, and decision makers.
- Provide accurate Client Materials, requirements, business rules, test data, acceptance criteria, compliance objectives, and legal/compliance assumptions.
- Review Deliverables, product outputs, evidence, reports, recommendations, and notices promptly.
- Maintain appropriate backups of Client systems and data.
- Maintain its own policies, controls, security program, privacy notices, compliance program, audit relationship, and legal obligations.
- Obtain all consents, licenses, approvals, and rights required for Provider to use Client Materials.
- Keep credentials, secrets, tokens, and access controls secure.
- Configure, secure, monitor, and maintain Client systems, repositories, identity providers, cloud accounts, payment accounts, admin accounts, production environments, backups, encryption settings, and access policies unless an Order expressly assigns a specific task to Provider.
- Remain responsible for all activity under Client accounts, API keys, tokens, service accounts, Organization Licenses, Registered Devices, projects, repositories, dashboards, and payment accounts, whether authorized or unauthorized, except to the extent caused by Provider's willful misconduct.
- Tell Provider before providing Regulated Data.

- Avoid using the Services or Products for unlawful, deceptive, abusive, infringing, unsafe, or high-risk purposes.
- Keep billing, legal, technical, security, admin, and notice contacts accurate and current.
- Cooperate with reasonable information requests from Provider, auditors, cloud providers, payment processors, communications providers, regulators, law enforcement, and other infrastructure providers when the request relates to Client's use of the Services or Products.

Client delays, missing information, inaccurate assumptions, account restrictions, unavailable personnel, third-party issues, or late approvals extend timelines and may increase fees.

7A. Licensing Units, Registered Devices, and Product Leases

This Section applies to every Product. The product-specific terms in Sections 8, 9, and 9A add to it and do not replace it.

bug, witness, and peachfuzz are licensed by Organization License. Their published subscription prices are flat for Client's organization and are not multiplied by users, repositories, projects, cores, commands, or Registered Devices. Where a plan is described as covering unlimited machines, Provider does not cap the number of Registered Devices under that Organization License. Every device must still be registered, and the license covers only Client and Client's authorized users. A signed Order may state a device cap for a custom, offline, self-hosted, abuse-remediation, or specially priced deployment.

Purchase activates the Organization License on Client's account; it does not activate an unregistered binary. Client downloads the Product, runs its register command, and supplies the Registration Token obtained from Client's authenticated account. The Product generates its device signing key on that device and sends the Registration Token through encrypted transport to Provider's control plane together with the Product's validated registration request, device identity, and device public key. The device private key never leaves the Registered Device. Provider validates the account, payment and trial state, Product, plan, entitlement, token, device identity, device public key, build identity, wire revision, and applicable device rules before issuing the signed device credential

and first signed Product Lease. A Product must not log, display, embed in evidence, or transmit a Registration Token anywhere except the registration request for which it is required.

After successful registration, the Product keeps the device credential and signed Product Lease and removes the Registration Token from process memory; it does not write that token to Product state. Registering another device requires Client to supply a valid Registration Token on that device. Ordinary renewal, payment recovery, plan upgrade, and self-service reactivation use the registered device credential and do not require Client to paste the Registration Token again unless the device itself must be registered again.

Provider's control plane is the authority for account, payment, trial, entitlement, Product, plan, device registration, Product Lease generation, upgrade, downgrade, refusal, reactivation, and for-cause revocation state. A Product enforces that state locally only after validating Provider's signature, Product identity, Registered Device identity, wire revision, generation, issuance time, and time boundaries. An unsigned response, transport status, cached webpage value, local configuration value, database row, or command-line flag is not licensing authority.

Every application-level response from Provider's control plane to an installed Product, including registration, check-in, custody, receipt, release, and upgrade responses, carries Provider Time and exactly one Product Status inside the signed response envelope. Network silence is not a Product Status and changes no signed state. A Product rejects the whole response if the signature, Provider Time, Product Status, response kind, revision, request nonce, Product identity, or Registered Device binding is absent, invalid, or outside the exact closed contract compiled into that release.

Provider Time for one Registered Device never moves backward. After validating the response, the Product advances its authenticated Provider Time high-water mark and uses that observation with its local clock to detect rollback and evaluate signed absolute boundaries. Provider Time is information, not additional authority: it cannot extend a Product Lease, move a next-contact boundary, create custody, or override a refusal or revocation.

Each installation must be activated against Client's account before it creates new licensed work. On activation, Provider issues a Product Lease to that Registered Device, and the Product Lease is valid only on the device it names. Copying, moving, restoring from backup, or sharing a Product Lease does not license any other device, and the Product will refuse new licensed work on a device its Product Lease does not name. Registering devices for, or otherwise making a Product available to, any person or entity other than Client and its authorized users is a breach of Section 30 whether or not a device limit is exceeded, and is a ground for immediate termination under Section 46.

Each Product may contact Provider's license service only at a Product-defined new-work boundary or scheduled check-in, and only when the signed decision held by the Product permits contact. While a Registered Device is online, ordinary check-ins occur at most approximately once per 24 hours. Opening, reading, auditing, exporting, or verifying records already created neither opens licensing state nor triggers a check-in. A check-in may transmit only the following categories of information:

- License and entitlement identity: the license key identifier, Organization License, Product, plan, activation state, and entitlement status.
- Device identity: a device identifier and device label for the Registered Device.
- Build identity: the binary's version and build hash, used to confirm the binary is an unmodified release build.
- Usage Window: bounded typed measurements since the last accepted watermark, including admitted command and work-unit counts, aggregate execution and CPU duration, result-class counts, queue or backlog counts, artifact and receipt counts, and freshness instants, together with the exact start and end of the window. Product-specific measurements are limited further below.
- Diagnostic and security signals: crash, error, activation, update, and abuse-prevention events about the binary and the check-in itself.

The categories above are the commitment. Provider may add, change, or remove individual fields within those categories as a Product develops, and the check-in payload is defined by a versioned wire contract that changes only within them.

Each check-in binds one Usage Window to its request nonce, previous watermark, Registered Device, Product, build, and lease generation. Provider validates and records that exact window idempotently and returns its accepted or rejected disposition and next watermark in the signed response. The Product clears acknowledged local usage only after validating that Provider accepted the exact window. Usage recorded while a check-in is in flight remains in the next window. Replaying an identical accepted window returns the same acceptance; reusing its identity with different measurements is a conflict and does not replace the accepted record.

Provider signs each licensing response as a grant, a recoverable refusal, or a for-cause revocation and binds it to the Product, entitlement, Registered Device, wire revision, generation, and issuance time. Provider may introduce and require a later wire revision for new licensed work. Provider does not maintain compatibility shims or promise to serve every historical wire revision indefinitely.

When an authentic released binary must upgrade, Provider returns a signed, recoverable upgrade-required decision under that binary's admitted revision and makes the authenticated replacement release available through the Product's upgrade path. The Product validates the selected release identity, digest, signature, platform, version, and policy before promotion and keeps the prior binary unless the replacement passes its required trial. An upgrade requirement does not alter records already created: those remain readable and verifiable with the released instrument and format that created them. A prepaid offline Product Lease is not shortened by a later wire revision during its signed prepaid term.

An upgrade, downgrade, reactivation, payment-state change, or other recoverable account transition takes effect through a newer signed decision at the next contact the current signed decision permits. The Product accepts only increasing generations and does not roll back to an older grant, refusal, plan, or entitlement. A plan change does not permit Provider to shorten a paid Product Lease already signed for the current paid period, except for a for-cause revocation permitted by this Agreement. Custody and retention consequences of a downgrade remain governed by Section 21B.2A.

The following exclusion is absolute, applies to every Product, applies to every automated Product channel and every version of every wire contract, and does not change with any release: bug, witness, and peachfuzz never transmit source code to Provider, and Provider's Product control plane never accepts source code. The same exclusion covers source-derived file contents, file paths, repository or branch names or identifiers, remote URLs, module paths, command arguments, issue or ticket titles or content, raw test or command output, corpus entries, generated inputs, crashing or reproduction inputs, stack traces, arbitrary evidence contents, secrets, credentials, personal information, protected health information, and other Client work product except for the exact source-free Custody Artifact fields Sections 8.1, 9.1, and 9A expressly admit, and except for the Corpus Entries and retained finding inputs that Section 9A.1 admits on the separate Cloud Evidence channel where Client has enabled it. Those two exceptions are the whole of what leaves a Registered Device beyond a license check-in, they are stated in the Sections named, and a category not named there is excluded. Provider will not add a Product field, configuration escape hatch, support flag, plan, or Order that carries source code through registration, check-in, usage, diagnostics, timestamping, custody, receipts, release, upgrade, Product support telemetry, or any other automated Product route.

Every Product wire body is a direct, versioned structure composed of named identities, closed enums, bounded numbers and durations, Provider Time and other typed instants, hashes, signatures, nonces, watermarks, and other fields this Agreement expressly permits. Product wire bodies do not contain generic metadata maps, arbitrary key-value attributes, untyped extension objects, free-form payload strings, opaque telemetry blobs, or catch-all byte fields. Provider documents the admitted field inventory and purpose so Client can inspect Product traffic and identify what each field means. Encryption in transit protects the exchange; it does not conceal a second undocumented payload.

Separately scoped custom Services may require Client to grant Provider repository access or provide source code under a signed Order. That is not Product telemetry or Product control-plane communication and does not weaken the Product exclusion above.

Provider uses check-in data solely for license administration, device registration, abuse prevention, billing integrity, service operation, and aggregate product planning under Section 35A. Check-in data is not sold and is not used to profile individual developers beyond license enforcement.

Entitlement is enforced locally before the Product creates new licensed work. Existing records remain permanently open, readable, auditable, exportable, and verifiable without evaluating a lease or contacting Provider. A signed grant carries the absolute activation, next-contact, ordinary-operation, and continuity boundaries selected by Provider. A recoverable refusal stops new licensed work and carries the earliest time at which the Product may ask again, so restoring payment restores access automatically at the next permitted new-work attempt or scheduled check-in. A for-cause revocation stops new licensed work and prohibits further licensing contact under that revoked decision. The Product accepts only an authentic decision for its Registered Device and never discards a newer refusal in favour of an older grant.

If the license service cannot be reached when a grant's ordinary-operation boundary is reached, the Product keeps full function until the continuity boundary Provider already signed, currently seventy-two hours later for ordinary online plans. The Product may attempt contact only at its Product-defined permitted new-work boundaries or scheduled check-ins and never before the signed next-contact boundary. That signed continuity interval absorbs network, firewall, proxy, or Provider outages; the binary does not invent or extend it locally. Disabling, blocking, intercepting, or spoofing a check-in in order to obtain function beyond a signed boundary is a breach of Section 30B.

If Provider ceases operating or the license service becomes permanently unavailable, an online Product continues only through the authority and continuity boundary Provider already signed, then stops creating new licensed work. No binary contains a hidden shutdown release, perpetual fallback, unsigned override, or local rule that can extend that authority. Existing bug and witness records remain readable, auditable, exportable, and verifiable as stated above; peachfuzz records already held on Client's systems remain Client's own. A prepaid offline Product Lease remains valid through its signed prepaid term. Provider's

operational wind-down, if one is possible, may issue newer signed decisions but cannot be promised in advance and is not authority a Product may assume.

Provider may revoke a Product Lease before the end of its term only on a ground stated in Section 46 or for breach of Section 30. Provider does not revoke a Product Lease because Client cancelled, because a plan will not renew, or because a payment was missed. A refusal, cancellation, non-renewal, or ordinary nonpayment is not a revocation. Cancellation and later account changes do not shorten authority Provider already signed. Cancellation is governed by Section 21B.2B, which leaves a paid period running to its end, and nonpayment is governed by the ladder in Section 21B.2.

Offline prepaid Product Leases use the same signed grant contract. Provider selects absolute activation, ordinary-operation, next-contact, and continuity boundaries covering the prepaid term so that the Product performs no check-in during that term. There is no separate offline lease format or local policy authority. Offline Product Leases remain bound to their Registered Devices and remain subject to Sections 30 and 30B in full.

7B. Custody Uploads, Validation, and Receipts

This Section applies only where the Order or published plan includes custody. A license check-in under Section 7A never carries a Custody Artifact. Custody uses a separate, explicit submission flow controlled by the Product terms, this Section, and the Privacy Policy.

Before an upload, the Product requests a short-lived upload authorization from Provider. Provider issues that authorization only after validating the account, Organization License, Product, plan, Registered Device, Product Lease, wire revision, artifact kind, artifact identity, declared digest, declared byte size, expiration, and server-issued nonce. The authorization is bound to that exact request and nonce, permits creation of one object only, and cannot authorize a replacement or a different object.

The upload authorization and its object-storage URL are bearer secrets. The Product may hold them only for the bounded transfer, must not log, display, embed in evidence, or persist them as completed Product state, and must discard them when the transfer reaches a terminal state or the authorization expires.

Provider stores the authorization's identity, one-way verifier, bounds, state, and audit history rather than a reusable plaintext URL.

The Product uploads the Custody Artifact through encrypted transport directly to Provider's designated object storage. Upload authorization does not mean acceptance. After upload, Provider validates the stored object's identity, size, digest, format revision, required signatures, entitlement, and artifact-kind rules before accepting it. Provider rejects an incomplete, expired, conflicting, malformed, oversized, wrongly signed, wrongly entitled, or otherwise invalid upload. A retry of the same valid artifact converges on the same result; a different artifact presented under the same identity is a conflict and is not permitted to overwrite the first.

After validation, Provider records the accepted artifact in Client's private account data and issues a signed receipt bound to the Product, account, Organization License, Registered Device, artifact identity, artifact kind, digest, byte size, format revision, acceptance time, storage identity, retention class, and receipt generation. The Product must validate that receipt before treating custody as complete. A transport response, upload completion, database write, dashboard display, or unsigned acknowledgement is not a custody receipt.

Provider's account database stores the validated metadata and state needed to operate custody, retrieval, receipts, retention, billing, abuse prevention, and Client's private dashboard. The object store holds the accepted Custody Artifact. The database is not the authoritative copy of the artifact, and the object store does not determine entitlement or legal state. Provider does not mark an artifact accepted, retained, published, or retrievable until the owning state has passed the validation required at that boundary.

Provider's systems may process a Custody Artifact automatically to validate, store, retrieve, export, and verify it. Provider personnel will not open, render, or inspect its contents except when Client expressly asks Provider to do so for a support request, a court orders Provider to do so, or applicable law compels Provider to do so. Where law permits notice, Provider will notify Client before producing or inspecting an artifact in response to legal process and will give Client a reasonable opportunity to seek protective relief. Where a protective order or equivalent relief is available,

Provider will take reasonable steps to seek it rather than treating the request as routine, and Section 48A applies to Provider's costs and time in doing so. Provider does not promise to defeat valid legal process, and no custodian can. Routine infrastructure access, integrity checks, replication, backup, encryption, and automated validation do not authorize personnel to review the artifact's substantive contents.

Provider may expose aggregated or de-identified product statistics under Section 35A. Provider will not make Client's identity, repository or project identity, findings, Custody Artifacts, evidence metadata, or account statistics public without Client's explicit authorization for the exact public field or publication. A plan's reference to a verification page means the Verification Page defined in Section 3: a capability-controlled path Client generates and controls, disclosing only the record the link names. It is not a public listing and Provider publishes nothing on it, unless the Order expressly identifies information Client chose to publish.

Custody begins only when Provider has accepted the artifact and issued the signed receipt. Client remains responsible for keeping its own authoritative local records and for confirming that the Product received and validated the receipt. Section 21B governs the Retention Lease after acceptance.

When Client upgrades from a no-custody plan or a shorter custody plan, the Product may submit an existing local artifact only if it was authentically created by that Product, satisfies the current plan's closed artifact contract, falls within the new plan's custody window, and passes the same validation as a newly created artifact. The signed receipt distinguishes the artifact's occurred-at time from Provider's acceptance time; an upgrade never backdates Provider's custody. Provider does not promise to reconstruct, convert, or accept local material that was never created in the required form.

8. Product-Specific Terms for bug

bug is a software development workflow and proof-of-fix system designed to support high-quality code, agent-readable work, compiler-visible contracts, traceable remediation, and evidence-driven development.

Client acknowledges:

- bug is a development tool and workflow aid, not a guarantee that software is defect-free, secure, compliant, profitable, available, or suitable for any specific production environment.
- bug depends on Client's repositories, commands, tests, configuration, environment, permissions, user inputs, and operational discipline.
- Results, reports, tickets, tests, and evidence produced by bug must be reviewed by qualified humans before reliance.
- Provider does not guarantee that every defect, regression, vulnerability, misconfiguration, legal risk, architectural flaw, or operational risk will be found.
- Client remains responsible for release decisions, production deployment, security review, code review, backups, incident response, and business outcomes.

Unless a signed Order expressly states otherwise, bug is licensed, not sold, and no ownership interest in bug or its source code transfers to Client.

8.1 bug Licensing Units and Check-In Counters

Section 7A governs bug's Organization License, device registration, Product Lease, check-in categories, continuity period, and offline operation. This Section states what is specific to bug.

bug is licensed by Organization License. Provider does not cap the number of Registered Devices under a published bug subscription unless the Order expressly states a cap. Each Registered Device holds its own Product Lease naming that device.

bug's Usage Window may contain only compiler-defined bug command and operation enums; invocation, record-created, closure, artifact, and receipt counts; aggregate execution duration; typed Product error classes; freshness instants; exact window boundaries; and the accepted watermark. It never contains a bug identity, title, description, issue or ticket field, test name or output, proof row, repository fact, command argument, or other work-product content. The absolute exclusion in Section 7A applies to every field of every release.

The bug Solo plan has no custody. Provider receives license check-ins under Section 7A and holds no bug Custody Artifact under that plan.

The bug Attested plan permits custody of a source-free closure artifact for up to one year while Client remains paid and in good standing. The bug Archive plan permits the same custody for up to five years while Client remains paid and in good standing. A qualifying prepaid Archive Order permits custody and a signed offline Product Lease for the exact prepaid term, which may be from one to five years as the published Order states.

A bug Custody Artifact may contain only the versioned closure record and verification material the Product defines: a random repository identifier that is not derived from a repository name, path, URL, or module; the operation and closure digests; the Merkle root or equivalent batch commitment; Product and schema revisions; the occurred-at time; the Registered Device and writer signing-key identifiers; the Product signature; Provider's countersignature; timestamp receipts; and the minimum verification metadata required to validate those values. It never contains source code, file contents or paths, repository or branch names, remote URLs, module paths, issue or ticket identity or content, bug titles or descriptions, test names or output, commands or arguments, proof rows, diffs, commit messages, secrets, credentials, or other Client work product.

Archive is the same bug binary and evidence format under a different custody and Product Lease policy. A prepaid Archive Product Lease performs no license check-ins during its signed term. It is not a second binary, a different key format, or a feature paywall.

9. Product-Specific Terms for witness

witness is a testing, evidence, and audit-readiness support system intended to help companies generate, organize, and validate technical evidence for security, compliance, and certification workflows.

Client acknowledges:

- witness is not a CPA firm, auditor, law firm, compliance certification body, attestation provider, Qualified Security Assessor, penetration testing firm, or regulator.
- Provider does not provide legal, accounting, tax, audit, attestation, certification, regulatory, privacy, security certification, or public accounting advice.

- witness may help prepare evidence for frameworks such as SOC 2, ISO 27001, HIPAA, HITRUST, CMMC, PCI DSS, FedRAMP, GDPR, PIPEDA, or internal vendor reviews, but Provider does not guarantee that Client will obtain, keep, pass, renew, or satisfy any certification, audit, attestation, procurement review, regulator review, customer review, insurance review, or security questionnaire.
- witness outputs depend on Client's controls, policies, procedures, systems, code, tests, logs, personnel, vendors, audit scope, configurations, and evidence accuracy.
- Client and its auditors, lawyers, compliance advisors, security advisors, and management are solely responsible for determining whether evidence is sufficient for any certification, audit, legal obligation, or business purpose.
- witness does not replace independent audit procedures, management assertions, control ownership, legal review, risk assessment, vulnerability management, security monitoring, or incident response.
- Client owns its control design, control operation, control evidence, management assertions, auditor relationship, remediation decisions, vendor questionnaire answers, trust-center publications, and certification scope. No auditor, regulator, customer, insurer, investor, marketplace, or other third party may rely on witness outputs unless Provider signs a separate written reliance agreement.

Custody of evidence by Provider is a paid service governed by Section 21B, including Section 21B.4, which states what happens to evidence when an account is cancelled or lapses. Client's protection in a dispute years later is the evidence Client exported and holds itself, which is designed to be verified independently of Provider, not Provider's continued custody of a copy.

Unless a signed Order expressly states otherwise, witness is licensed, not sold, and no ownership interest in witness or its source code transfers to Client.

9.1 witness Licensing Units and Check-Ins

Section 7A governs witness's Organization License, device registration, Product Lease, check-in categories, continuity period, and offline operation.

witness is licensed by Organization License. Provider does not cap the number of Registered Devices under a published witness subscription unless the Order expressly states a cap. The custody tier Client selects determines the Retention Lease under Section 21B and does not change the licensing unit.

witness's Usage Window may contain only compiler-defined witness command, profile, result, and operation enums; command, run, result-class, artifact, timestamp, and receipt counts; aggregate execution and CPU duration; queue or backlog counts; typed Product error classes; freshness instants; exact window boundaries; and the accepted watermark. It never contains a repository, package, test, benchmark, profile-instance, file, finding, output, command argument, evidence-content, or other customer-controlled name or value. The absolute exclusion in Section 7A applies to every field of every release, and applies in addition to Section 4 of the Privacy Policy, which governs the separate source-free custody and timestamp records witness sends when Client uses those features.

The witness Local plan has no custody. Bronze permits custody for up to one year, Silver for up to three years, and Gold for up to ten years, in each case only while Client remains paid and in good standing. A witness Custody Artifact is the sealed, source-free custody projection produced on Client's machine. It may contain only compiler-defined Product, release, schema, policy, profile, tool, and result enums; opaque run and installation identities; bounded counts and durations; ledger, manifest, artifact and report commitments; hashes; timestamp receipts; run attestations; checksums; signatures; and verifier material. It never contains customer-controlled free text, source code, source-derived file contents, names or paths, raw test or command output, reproduction inputs, corpus or crashing inputs, secrets, credentials, production data, personal information, protected health information, full private datasets, or the local human-readable report itself. The Product validates the projection against its closed custody allowlist before submission. Client keeps the complete local bundle and report; the accepted projection and signed receipt prove which local bundle existed without sending its contents to Provider.

9A. Product-Specific Terms for peachfuzz

peachfuzz is a continuous fuzzing and effort-recording daemon that searches Client's own code on Client's own hardware and produces signed records of the search effort performed.

Client acknowledges:

- peachfuzz is a testing tool and workflow aid, not a guarantee that software is defect-free, secure, compliant, or suitable for any specific production environment.
- peachfuzz depends on Client's code, corpus, configuration, hardware, scheduling, and operational discipline, and the effort it records reflects the compute Client provides to it.
- Provider does not guarantee that any defect, crash, vulnerability, or edge case will be found. An absence of findings is a record of effort spent, not evidence that no defect exists, and must not be represented as the latter.
- Results and effort records produced by peachfuzz must be reviewed by qualified humans before reliance, and Section 10 applies to them.
- Client remains responsible for release decisions, production deployment, security review, code review, incident response, and business outcomes.

peachfuzz is licensed by Organization License. Provider does not cap the number of Registered Devices under an Organization License for peachfuzz unless the Order states a cap. Section 7A applies in full, including the requirement that every device be registered and the prohibition on making the Product available to any person or entity other than Client and its authorized users.

peachfuzz's Usage Window may contain only compiler-defined peachfuzz command, scheduler-action, run-state, and outcome enums; command, slice, run, target-count, candidate-count, outcome-class, artifact, and receipt counts; aggregate execution and CPU duration; queue or backlog counts; typed Product error classes; freshness instants; exact window boundaries; and the accepted watermark. It never contains repository, package, target, corpus, candidate, finding, input, stack-trace, path, output, command-argument, raw-run-record, or other customer-controlled names or content.

peachfuzz has no read-only state. Because it is a continuous service that produces new records rather than a reader of records already made, the restriction described in Sections 21B.2 and 21B.2B stops peachfuzz entirely rather than reducing it. Records already written to Client's own systems remain Client's own, readable and verifiable without Provider, as Section 21B.2B provides.

Where Client's plan includes custody, Section 7B governs submission and receipts and Section 21B governs Provider's retention of the independently held copy. The peachfuzz Local plan has no custody. Attested permits custody of signed effort evidence for up to one year, and Archive permits custody of signed effort evidence for up to five years, in each case only while Client remains paid and in good standing.

A peachfuzz Custody Artifact may contain only versioned, signed effort and finding metadata: Product and schema revisions; account, Organization License, Registered Device, machine-key, run, and target identities that are random or content-addressed and do not disclose Client naming; counting-window boundaries; bounded counters for invocations, CPU effort, elapsed run state, target coverage, candidate counts, unique finding counts, and outcome classes; content digests; signatures; timestamps; and the minimum verification metadata required to validate those values. It never contains source code, file contents or paths, repository or branch names or identifiers, remote URLs, module paths, target names, command arguments, corpus entries, generated inputs, crashing inputs, reproduction inputs, stack traces, test output, raw run records, secrets, credentials, personal information, protected health information, or other Client work product. Corpus Entries and retained finding inputs are not Custody Artifact fields. Where Client has enabled Cloud Evidence they travel on the separate channel Section 9A.1 defines, and where Client has not enabled it they never leave Client's systems at all.

Within a Custody Artifact, finding metadata means counts and content-addressed identities only. The artifact records that a finding exists and when it was first and last observed, and carries nothing from which the defect could be reconstructed. Whether Provider also holds the input that produced a finding depends entirely on Cloud Evidence: Section 9A.1 governs that, it is off unless Client turns it on, and it is available only on the plans whose published terms include it.

9A.1 Cloud Evidence: Corpus Exchange and Finding Backup

Why this feature exists is stated first, because it explains everything that follows. A coverage-guided fuzzer works by generating an enormous number of inputs, almost none of which are interesting, and keeping the few that reach program behaviour nothing has reached before. The search is only worth running if it runs for a long time, and it is only worth running on more than one machine if those machines do not spend that time re-searching ground another machine has already covered. Sharing retained Corpus Entries between Client's own Registered Devices is what makes the second machine worth switching on. Without it every machine starts from nothing, and the compute Client is paying for duplicates the search instead of extending it.

Cloud Evidence is off by default and is not switched on by buying a plan. Client enables it explicitly in the Product's validated configuration, and only on a plan whose published terms include it. The peachfuzz Local plan has no Cloud Evidence. While it is off, nothing in this Section leaves a Registered Device and the license check-in in Section 7A is the only Product traffic.

While Cloud Evidence is on, each Registered Device may upload the following to tenant-private storage, and other Registered Devices of the same Client may retrieve it:

- Corpus Entries retained because they reached new coverage and not previously uploaded.
- Retained finding inputs, meaning the exact input bytes that produced a retained finding, held separately from the active corpus so a known failure is not fed back into ordinary fuzzing.
- The signed Custody Artifact described above, together with its verification material.

What those bytes are is stated plainly, because the accuracy is the whole of Client's protection. A Corpus Entry is a byte string. It is predominantly machine-generated, produced by the fuzzing engine mutating earlier inputs, and it is retained for the code path it reached rather than for anything it means. It is not source code, a file or repository path, a repository or branch name, a module path, a command argument, a credential, a secret, or raw process output, and none of those are uploaded on this channel or any other. But a Corpus Entry descends from the seed inputs Client

placed in Client's own repository, and a retained finding input is by definition the data that caused a failure. Either can therefore carry fragments of whatever Client seeded, and Provider states that here rather than leaving Client to infer it.

Client is responsible for what Client seeds. Before enabling Cloud Evidence, Client should consider whether its seed corpora are built from real production data, personal information, or Regulated Data, because uploads derived from those seeds may carry parts of them. Section 26 applies in full, and Client must not enable Cloud Evidence for a project whose corpus contains Regulated Data unless the applicable Order and any required addendum expressly permit it.

Uploads are encrypted in transit and encrypted at rest, are held in storage private to Client's tenant, and are content-addressed and create-only: an identical retry converges on the same object, and a different object presented under the same identity is a conflict rather than a replacement.

Provider holds the encryption keys and is therefore technically able to read an uploaded object. Provider does not. Provider's systems process uploads automatically to store, deduplicate, distribute to Client's own Registered Devices, retrieve, and export them, and Provider personnel will not open, render, or inspect their contents except in the three circumstances Section 7B already states: Client expressly asks Provider to do so for a support request, a court orders Provider to do so, or applicable law compels Provider to do so. The notice, protective-relief, and cost provisions of Sections 7B and 48A apply in the same way.

Because Provider is able to read these objects, valid legal process served on Provider can reach them. That is the honest consequence of the feature, it is the reason the feature is off by default and stated here rather than in a support article, and Client should weigh it before enabling Cloud Evidence.

Cloud Evidence is retained under the Retention Lease in Section 21B for the window the plan states, currently one year on peachfuzz Attested and five years on peachfuzz Archive, in each case only while Client remains paid and in good standing. Section 21B.4 applies in full: cancellation ends custody.

Client's local copy remains authoritative throughout. Nothing in Cloud Evidence is required to run peachfuzz, to reproduce a finding, to read a run record, or to verify effort already recorded on Client's own disk.

Where Client's plan does not include custody, Provider holds no peachfuzz Custody Artifact and the storage, retention, expiry, and deletion provisions of Section 21B have nothing to act on.

Unless a signed Order expressly states otherwise, peachfuzz is licensed, not sold, and no ownership interest in peachfuzz or its source code transfers to Client.

10. No Professional Advice

Provider does not provide legal, accounting, audit, tax, financial, investment, insurance, medical, regulatory, public accounting, or certification-body services. Any templates, controls, tests, reports, policies, checklists, evidence packages, comments, recommendations, or product outputs are technical and operational aids only.

Client bears sole responsibility for every legal, audit, certification, regulatory, insurance, securities, tax, privacy, employment, health-information, financial-services, public-procurement, and other regulated determination made using a Deliverable or Product output. No Deliverable or Product output is professional advice or transfers that responsibility to Provider.

11. No Guarantee of Business, Security, Compliance, or Certification Outcomes

Provider does not guarantee:

- Bug-free, error-free, uninterrupted, secure, vulnerability-free, or incident-free software.
- Specific SEO ranking, ad performance, conversion rate, revenue, fundraising, valuation, customer growth, uptime, latency, scalability, marketplace approval, app-store approval, procurement approval, or business result.
- Compliance with any law, regulation, standard, policy, contract, security framework, certification, audit, attestation, or customer requirement.

- That any website, app, API, Product, report, evidence package, test, recommendation, or workflow will satisfy a third party.
- That any AI, automation, agent, compiler, test, lint, scan, or analysis result is complete, current, or correct.

All warranties are limited to those expressly stated in this Agreement or a signed Order.

12. Project Management and Communications

Provider will use commercially reasonable efforts to communicate project status through the channels and cadence stated in the Order. If no cadence is stated, Provider may choose a reasonable cadence based on project complexity.

Client must identify one authorized decision maker. Provider may rely on instructions, approvals, credentials, access grants, and acceptance from that person unless Client gives Provider written notice of a replacement.

12A. Communications, Records, and Conduct

Provider keeps a record of the project. Client agrees that communications between the Parties relating to an Order may be retained by Provider as part of that project record and kept for the periods described in the Privacy Policy. This includes email, messaging applications such as WhatsApp, SMS, chat, ticket and pull request comments, voice and video calls, voicemail, and notes of in-person meetings.

Provider may record or transcribe calls and meetings for that record. Where Provider records the audio or video of a call or meeting, Provider will say so at the start of it, and Client may decline, in which case Provider may keep written notes of the same conversation instead.

The record exists so that what was asked for, agreed, approved, refused, and delivered can be established later without argument, and so that a disagreement is settled by what was actually said rather than by what either Party remembers. Either Party may use it for that purpose, including in a dispute, an audit, an invoice dispute, or a proceeding.

Keeping a record does not change what is binding. Under Sections 4, 6, and 15, an informal message, call, or meeting does not create scope, a warranty, an acceptance, a service level, a deadline, a price, or an Order, however clearly it was recorded. Only a written change order or a signed Order does that. Client may not rely on a retained message as an approval of work that no Order describes.

Provider will make reasonable efforts to work with Client's preferred communication channel, cadence, and working style, and to understand and align with the values, priorities, and intent behind a project. Reasonable efforts are exactly that. They are not a commitment to any particular channel, application, response time, availability, meeting frequency, working hours, or way of working, they do not entitle Client to direct how Provider works, and Provider is not bound by a preference that is not stated in the Order.

Conduct is part of the working relationship. Provider may decline to quote for, accept, renew, or continue any further Order, and may end a current engagement where Section 46 applies, on the basis of how Client, its personnel, or its representatives conduct themselves in these communications, including abuse, threats, harassment, discrimination, dishonesty, misrepresentation of what was agreed, repeated refusal to use the change process in Section 15, or persistent conduct that makes the working relationship unworkable. Provider is not required to give a reason for declining future work, and declining future work is not a breach of this Agreement.

13. Delivery Dates and Dependencies

Delivery dates are estimates unless the Order expressly states that a date is a fixed deadline. Delivery dates depend on timely Client cooperation, third-party availability, payment, stable requirements, and access to required systems.

If Client delays a dependency, requests changes, changes priorities, withholds payment, fails to provide access, or misses an approval deadline, Provider may extend the schedule and charge for idle time, restart time, remobilization, or additional work.

14. Expedited Work

Expedited delivery, rush work, emergency work, after-hours work, weekend work, and priority support are available only if Provider agrees in writing. Expedited work may require additional fees and may require scope reduction, changed milestones, or changed acceptance criteria.

Expedited fees are non-refundable unless a signed Order expressly states otherwise.

15. Change Control

Changes to scope, features, designs, integrations, APIs, data models, hosting, compliance objectives, testing requirements, controls, evidence requirements, security assumptions, or acceptance criteria require written approval by Provider.

Provider may refuse a change request if it creates legal risk, security risk, unreasonable support burden, architectural risk, quality risk, timeline risk, payment risk, or conflict with Provider's standards. Provider may refuse for any other reason, and refusing a change is not a breach of this Agreement, a failure to perform, or grounds to withhold payment for work already performed.

Approved changes may alter price, timeline, dependencies, acceptance criteria, support obligations, and maintenance fees. No change is approved, and no work on it begins, until both the scope and the new price are agreed in writing.

A change requested late is still a change. Direction that reverses an earlier approval, revisits an accepted Deliverable, introduces a new audience, brand, business rule, integration, platform, or design direction, or asks for work to be redone to a different taste is out of scope regardless of when it arrives, how small it appears, how close the project is to launch, or how strongly Client feels about it. It requires a new written approval and a new price before Provider starts it, and Provider may decline it outright.

Accepted work stays accepted. Provider is not required to reopen, redo, restyle, or rework a Deliverable that has been accepted or deemed accepted under Section 18. Doing so is new work under a new Order at a new price. Repeated, contradictory, or reversing direction is billable at Provider's then-current rate whether or not it results in a change order.

Provider decides how the work is done. Subject to delivering what the Order describes and meeting the acceptance criteria stated in it, Provider selects and may change the methods, tools, languages, frameworks, libraries, hosting arrangements, internal processes, subcontractors, sequence of work, and working schedule it uses, as Section 50 also provides. Client's preference about how the work is done is not an acceptance criterion unless the Order states it as one.

16. Revisions

Unless an Order states otherwise, custom Services include two rounds of reasonable revisions limited to the agreed scope. A revision round must be consolidated, specific, and delivered by Client in writing.

Additional revisions, contradictory feedback, late feedback, redesigns, new features, changed business rules, changed copy, changed integrations, changed acceptance criteria, or changes after acceptance are out of scope and billable.

17. Testing and Quality

Provider will use commercially reasonable testing practices appropriate to the Order. Testing may include functional tests, integration tests, user acceptance support, accessibility checks, security-oriented checks, performance checks, linting, static analysis, CI checks, compiler checks, or Product-specific evidence checks.

Testing does not guarantee that all defects, vulnerabilities, regressions, browser issues, device issues, accessibility issues, compliance issues, edge cases, or third-party failures will be found.

Client is responsible for user acceptance testing, business-rule validation, production readiness decisions, and verifying that Deliverables meet Client's operational, legal, compliance, and security needs.

18. Acceptance and Deemed Acceptance

Unless an Order states otherwise, Client has five business days after delivery to accept or reject a Deliverable in writing.

A rejection must identify specific material nonconformities against the signed Order. Provider will use commercially reasonable efforts to correct valid material nonconformities.

A Deliverable is deemed accepted if:

- Client does not provide a valid written rejection within the review period.
- Client uses the Deliverable in production or for business operations.
- Client makes the Deliverable public.
- Client provides approval in writing.
- Client prevents final testing or deployment through delay, withheld access, or missing inputs for more than ten business days after Provider requests them.

Acceptance does not waive unpaid fees, license restrictions, confidentiality obligations, or Provider Background IP rights.

19. Fees

Client will pay the fees stated in the applicable Order or invoice. Fees may include fixed project fees, deposits, milestone fees, hourly fees, subscriptions, license fees, hosting fees, maintenance fees, support fees, domain fees, SSL/TLS fees, usage-based fees, overage fees, third-party expenses, and taxes.

Unless an Order states otherwise:

- Deposits are due before work begins.
- Subscription fees are due in advance.
- Invoices are due on receipt.
- ALL SALES ARE FINAL. No refunds, no credits, no cooling-off period, no satisfaction guarantee, and no partial refund for unused time, unused licenses, or unused capacity. Client does not get money back for changing its mind, changing direction, changing priorities, losing budget, losing an internal sponsor, disliking the result, hiring someone else, or deciding it no longer wants the work.

- Where Provider's own work is genuinely nonconforming, Client's exclusive remedy is re-performance under Section 36: Provider fixes it. Provider may instead elect to refund the fees paid for that specific nonconforming portion, and Section 42 lets Provider elect to refund prepaid unused fees to resolve an infringement claim. Those elections belong to Provider alone. They are Provider's choice of how to make something right, not a right for Client to demand money back.
- The single exception, and it applies only where Provider walks away: if Provider terminates a custom Services Order for convenience while Client is not in breach, Section 45 returns the prepaid amount for work Provider has not performed. No other section of this Agreement gives Client a right to demand money back.
- The Initial Trial in Section 19A lets Client cancel before any fee is charged. That is a cancellation, not a refund.
- Fees are non-refundable once paid.
- Taxes, duties, withholding, bank fees, chargeback fees, and currency conversion fees are Client's responsibility.
- Client may not withhold, offset, or reduce payment because of unrelated disputes.
- Usage measurements, registered-device counts, quota consumption, license activations, storage use, API calls, overages, and other Product billing calculations are determined by Provider's records unless Client shows a manifest calculation error.
- Minimum commitments, prepaid subscriptions, license terms, reserved capacity, discounted packages, and accepted Orders are non-cancellable and non-refundable except to the extent a signed Order expressly states otherwise. For clarity, ending a monthly plan under Section 44 is not a cancellation of the period already paid for: it stops the next renewal, the current period runs to its end with full use, and nothing is refunded for it.
- Any invoice dispute must be raised in writing within thirty days after the invoice date, with reasonable detail. Client must timely pay all undisputed amounts while the dispute is reviewed.

19A. Initial Trial

Provider may offer a one-time initial trial of an eligible Product subscription (the "Initial Trial"). Unless the Order or the checkout page states a different period, the Initial Trial runs for thirty consecutive days beginning on the date Client first activates the subscription, whether or not Client uses the Product during that period.

The Initial Trial applies only to Product subscriptions that Provider designates as trial-eligible at checkout. It does not apply to custom Services, professional services, deposits, milestone work, hosting, domains, SSL/TLS certificates, third-party services, enterprise or offline licenses, paid-up archives, reserved capacity, prepaid or discounted packages, minimum commitments, or any Order that states it is not trial-eligible.

Unless the Order or the checkout page states otherwise:

- Provider may require a valid payment method before the Initial Trial begins, and may authorize, verify, or place a temporary hold on that payment method.
- Provider may require Client to confirm its business or organization name and its business, non-consumer purpose under Section 2 before the Initial Trial begins.
- The Initial Trial converts automatically to a paid subscription at the end of the trial period, at Provider's then-current rate for the selected plan, and renews under Section 44 unless Client cancels before the trial period ends.
- Client may cancel at any time before the end of the Initial Trial through the account dashboard or by written notice under Section 59. Cancellation takes effect at the end of the trial period, and no subscription fee is charged for that period.
- Once the Initial Trial ends and the subscription converts, all fees are governed by Sections 19 and 20 and are non-refundable. Cancelling after conversion stops the next renewal; it does not refund or credit the current period.
- Third-party charges, taxes, usage-based fees, overage fees, and out-of-scope work incurred during the Initial Trial remain payable even if Client cancels.

The Initial Trial is limited to one per Product per Client, not one per plan, account, user, Registered Device, project, or affiliate. A Client that has used bug's Initial Trial may later use witness's or

peachfuzz's Initial Trial if that Product is trial-eligible, but may not obtain another Initial Trial for the same Product by selecting a different plan or by creating additional accounts, entities, email addresses, domains, payment methods, devices, projects, or affiliates, or by cancelling and re-subscribing. Provider may refuse, shorten, suspend, or terminate an Initial Trial, and may charge Client for the trial period at the then-current rate, if Provider reasonably determines that Client has attempted to obtain another trial for the same Product, has breached this Agreement, or is using the Initial Trial abusively, unlawfully, or to circumvent fees.

During the Initial Trial the Product is generally available software, not a beta, preview, or evaluation feature. Sections 8, 9, 30, 30A, 30B, 36, 37, 39, and 41 apply in full during the Initial Trial. Section 38 does not apply to the Initial Trial, except that any beta, preview, or pre-release feature accessed during the Initial Trial remains governed by Section 38. Because no fees are paid during the Initial Trial, Provider's total aggregate liability for the Initial Trial period is capped as stated in Section 39.

Provider may change, limit, suspend, or discontinue the Initial Trial offer for future customers at any time. Doing so does not affect an Initial Trial already in progress.

20. Deposits, Milestones, and Non-Refundable Fees

Deposits reserve Provider capacity and are non-refundable. Milestone payments become due when the milestone is reached, whether or not Client has completed its internal review, unless Provider is the sole cause of the missed milestone.

Fees for completed work, accepted work, Product subscriptions, license keys, setup, onboarding, training, rush work, third-party services, domain purchases, SSL/TLS certificates, cloud services, hosting, maintenance, support retainers, and expenses are non-refundable to the maximum extent permitted by law.

If Client cancels or pauses work, Client remains responsible for work performed, committed costs, non-cancellable expenses, approved third-party costs, unpaid subscriptions, and any applicable kill fee.

21. Late Payment, Suspension, and Collection

Amounts not paid when due may accrue interest at the lesser of 2% per month, 24% per year, or the maximum rate permitted by applicable law, calculated from the due date until paid.

If payment is late, Provider may suspend Services, Products, hosting, support, maintenance, license access, deployments, deliverables, domain management, or account access until all overdue amounts are paid. Provider is not liable for losses arising from a suspension caused by nonpayment.

If recurring fees for website hosting, email services, domain management, maintenance, support, retainers, or other recurring services remain unpaid for forty-five days after the due date, Provider may disconnect, disable, suspend, or terminate the affected services. Reconnection is at Provider's discretion and requires payment of all overdue amounts plus a CAD $100 reactivation fee unless an Order states a higher reactivation fee.

This forty-five day rule does not apply to bug, witness, peachfuzz, or any other Product subscription. Those follow the ladder in Section 21B, which is the whole of what happens when a Product subscription goes unpaid. One service is governed by one clock, and the two do not overlap.

Client will reimburse Provider for reasonable collection costs, chargeback costs, bank fees, legal fees, arbitration fees, court fees, and enforcement costs incurred in collecting overdue amounts.

21A. Payment Processors, Chargebacks, and Merchant Risk

If Services or Products integrate with Stripe, Shopify Payments, banks, card networks, merchant acquirers, app marketplaces, or other payment processors, Client remains responsible for processor account approval, know-your-customer checks, prohibited or restricted business rules, payment method rules, reserves, holds, refunds, reversals, disputes, chargebacks, fraud, fulfillment, taxes, customer claims, and processor suspension or termination.

Provider is not liable for payment processor decisions, payment holds, declined transactions, account freezes, reserve requirements, processor underwriting, network fines, customer

disputes, chargebacks, tax reporting, settlement delays, or lost revenue caused by payment infrastructure unless a signed Order expressly assigns that risk to Provider.

If Client or Client's bank, card issuer, payment provider, representative, employee, contractor, or agent reports, disputes, reverses, claws back, reclaims, charges back, or flags a valid payment as fraudulent, suspicious, unauthorized, mistaken, duplicate, defective, or otherwise improper, Client must promptly reimburse Provider for the full invoiced amount, the full amount reclaimed, held, deducted, reserved, debited, or withheld by any bank, card issuer, payment provider, processor, or marketplace, all Stripe or other payment processor fees, the original payment processor fee, any lost non-refundable processing percentage, chargeback fee, dispute fee, retrieval fee, investigation fee, bank fee, reserve fee, currency-conversion cost, collection cost, legal fee, and reasonable administrative cost incurred by Provider.

The principle behind this Section is that Client restores Provider to the position Provider would have been in if the payment had been made and had not been reversed. Provider does not absorb any part of the cost of a reversal, including the part the payment processor keeps.

Processing fees are not returned when a payment is reversed. When Client pays by card, the processor deducts its fee from the amount Provider receives. When that payment is later charged back, the processor takes back the full gross amount from Provider and keeps the fee it already deducted, so Provider is out both the money and the fee. That retained fee is Client's cost under this Section, whether or not the processor itemizes it, whether or not it is recoverable by Provider, and whether or not the dispute is later resolved in Provider's favour.

Stated as arithmetic so there is nothing to interpret: on a reversed payment of CAD $10,000 carrying a three percent processing fee, Client owes the CAD $10,000 invoiced amount, the CAD $300 processing fee the processor retained, every dispute, representment, retrieval, investigation, bank, reserve, and currency-conversion fee charged to Provider in connection with the reversal, the minimum one-day time charge of CAD $4,400 set out below, the CAD $1,000 liquidated amount set out below, and

Provider's collection and legal costs. A payment that leaves Provider short of that total does not discharge the obligation and does not restore the account.

These amounts are written out here, with the arithmetic worked through, rather than left in a schedule or a support policy, so that Client sees what a reversed payment costs before agreeing to anything rather than after making one.

Any replacement payment must be grossed up so that Provider actually receives the full amount owing after any fee charged on that replacement payment. If Client pays again by card, Client owes the fee on that payment as well. Provider may require the replacement payment to be made by bank transfer or another method that carries no processing fee and cannot itself be reversed.

Client must also pay Provider for time spent investigating, responding to, documenting, disputing, reversing, reconciling, collecting, or remediating the payment report, dispute, reversal, chargeback, clawback, bank reclaim, processor reclaim, or related account restriction. That time is charged at CAD $550 per hour, or at Provider's then-current professional services rate if that rate is higher, with a minimum charge of one full working day of eight hours for each such event.

The minimum is a full day, and the Parties record here why they agreed on that figure.

This charge only arises where Client chose not to raise the matter with Provider first. Provider offers an invoice-dispute process that is free, immediate, and answered by the person who did the work. Instead of using it, Client tells its bank that a payment it authorized was fraudulent or unauthorized. The bank does not telephone Provider to ask. It opens an investigation into Provider, takes the money back, and gives Provider a deadline to prove that its own charge was legitimate.

What follows is not a day of light administration. Provider stops engineering, product development, marketing, sales, and delivery work for other clients, because the processor's deadline is fixed and does not move for Provider's schedule. Provider works through the processor's dispute console, contacts the processor and its own bank, assembles invoices, correspondence, delivery records, acceptance records, and access logs into a submission,

and contacts Client to establish what happened. None of that work produces anything. It is unproductive work, compelled at someone else's timing, defending an accusation of dishonesty that Client could have avoided by sending one email.

The Parties therefore agree that one working day is a conservative pre-estimate of what a single reversal costs Provider, that billing in shorter increments would not reflect what actually happens, and that the minimum is compensation for a real and foreseeable displacement rather than a penalty.

In addition, Client will pay Provider CAD $1,000 as liquidated damages for each payment that is charged back, reversed, reclaimed, or reported as fraudulent, unauthorized, or improper without Client first raising the matter through the invoice-dispute process in this Agreement.

That amount is separate from the time charge above and compensates Provider for no hour of work. It is the Parties' genuine pre-estimate, agreed when they entered into this Agreement, of the harm a payment dispute does to Provider's ability to accept payment at all: a dispute recorded permanently against Provider's merchant account, an increased dispute ratio measured against thresholds set by the card networks rather than by Provider, and the resulting risk of higher processing fees, rolling reserves, withheld settlements, additional underwriting review, and termination of Provider's ability to process card payments. That harm is caused by Client's report rather than by anything Provider did, it persists whether or not the dispute is later resolved in Provider's favour, and it cannot be measured precisely, which is exactly why a fixed amount is agreed in advance. The Parties agree it is reasonable in light of that harm, that it is not a penalty, and that it may be less than Provider's actual loss.

The two amounts cover different losses. One is the working time consumed, the other the damage to Provider's payment relationship, and neither duplicates the other. Both are in addition to the out-of-pocket amounts listed above, which are reimbursed at their actual cost.

This obligation applies whether the report, dispute, or reversal is made intentionally, carelessly, mistakenly, by an employee, agent, representative, or accountant of Client, or automatically by a bank or card-issuer fraud system acting on Client's account, because in each case the consequences to Provider are the same. It does not

apply where Client first raised the matter in writing through the invoice-dispute process and Provider failed to respond within a reasonable time.

Describing a valid, authorized payment as fraudulent or unauthorized is a statement made to Client's bank and to Provider's payment processor about Provider's conduct. Client is responsible for that statement and for its consequences, including the consequences that fall on Provider's merchant standing rather than on the disputed amount.

Where a payment is reversed, Provider may immediately suspend the affected Services, Products, accounts, and access under Section 21. Restoration requires payment in full of the reclaimed amount, the out-of-pocket amounts listed above, and the liquidated amount, and Provider may require that payment, and any future payment, be made by bank transfer or another method that cannot itself be reversed. Provider is not obliged to restore anything before those amounts clear.

If Client believes an invoice or payment is incorrect, Client must first use the invoice-dispute process in this Agreement and must not initiate a chargeback, fraud report, bank reversal, payment-provider dispute, or similar reclaim unless required by law or unless Provider has failed to respond to a proper written invoice dispute within a reasonable time.

21B. Retention Leases, Payment Lapse, and Wind-Down

This section says exactly what happens to Client's data if Client stops paying, and when it is deleted. It is stated in full here rather than left to a support policy, because it is the part of the arrangement most worth knowing before buying.

Custody applies to some Products and plans and not to others. bug Solo, witness Local, and peachfuzz Local have no custody. bug Attested and Archive, witness Bronze, Silver, and Gold, and peachfuzz Attested and Archive permit custody only of the Custody Artifacts their Product-specific terms define. Where Provider holds nothing, everything in this Section about storage, retention, expiry, and deletion has nothing to act on, and only the licensing terms and the payment ladder in Section 21B.2 apply.

Retention is a lease, not a vault. Published custody windows range from one year to ten years, and ten years is the longest window Provider publishes. The applicable Product-specific terms state each plan's window. That term is the maximum custody period available while the account remains paid, active, and in good standing, or while a separately purchased paid-up archive, legal hold, court order, law, or signed Order requires longer retention. It is not a prepaid guarantee that Provider will hold data for the full term regardless of payment, and buying a ten-year term does not oblige Provider to keep data for ten years after Client stops paying for it.

21B.1 How the Lease Works

Retained data is held in storage configured so that it cannot be deleted before a set expiry date, by Provider or by anyone else, until that date passes.

When an eligible plan is activated, Provider sets that expiry six months ahead. Each subsequent monthly payment extends it by one further month, so a paid account continuously holds a rolling window of approximately six months of undeleteable retention ahead of it. A payment covering a longer period extends the expiry by the period paid.

This cuts both ways, deliberately. Client always has the remaining window, up to approximately six months from the last payment, during which its data physically cannot be deleted, whatever else happens to the account, including a dispute. Provider does not carry a ten-year storage obligation bought with two months of payments.

Nothing is deleted before the expiry date on the storage, even after the notices below. If the expiry date falls later than a date stated in a notice, deletion happens when the expiry passes. Client should not rely on that: the notice dates are the dates to act on.

21B.2 What Happens When a Payment Is Missed

Each step below is preceded by an email to Client's billing or account contact, sent by Provider or by Provider's payment processor acting on Provider's behalf. Client is responsible under Section 7 for keeping that contact accurate, and a notice sent to the contact on file is effective whether or not Client reads it.

In this section, a missed payment means an invoice that remains unpaid after Provider's payment processor has finished its automatic retries for that invoice. A single invoice that is retried several times is one missed payment, not several. The third missed payment therefore means the third unpaid invoice, not the third failed attempt on one invoice.

On the day a payment fails, Client is notified and asked to update its payment method. The Products keep working normally. Provider's payment processor may also retry the payment automatically over the following days, and a retry that succeeds returns the account to good standing with nothing further required from Client.

Once the payment processor has finished its automatic retries for that invoice without success, and in any event no earlier than approximately seven days after the payment first failed, the Products stop doing new work and keep doing read-only work. witness stops accepting new runs, new evidence, and new timestamping, and continues to verify evidence already held. bug stops creating new records and reports, and continues to open, read, and audit records already created. peachfuzz stops, because it is a continuous service with nothing to read back.

The notice and deletion steps that follow apply only where Provider holds a Custody Artifact for Client. For bug Solo, witness Local, peachfuzz Local, and self-hosted deployments under Section 21B.5, Provider holds no Custody Artifact, so those steps have nothing to act on: the Product Lease restricts and resumes as described above and below, and no Client artifact held by Provider is affected either way.

From approximately thirty days after the failed payment, Provider sends a second notice stating that the account is unpaid, that data held on Client's behalf is scheduled for deletion in approximately sixty days, and that Client should export its data now. Export remains available through the available export method, subject to authentication, security controls, and legal restrictions.

On the third missed payment, Provider sends a third notice stating that the account is treated as closed, that permanent deletion will follow, and that Client should download everything it wants to keep. Provider stops extending the retention lease, and the data is deleted once the storage expiry date passes as described in Section 21B.1.

Client can put the account back in good standing itself, at any point before deletion, by signing in to its account on Provider's website and paying the overdue amounts. There is no reactivation fee on a Product subscription: the reactivation fee in Section 21 applies to hosting, email, domain management, maintenance, support, and retainers, and not to bug, witness, or peachfuzz. No support ticket, approval, or contact with Provider is required, and nothing has to be reissued by hand.

Restoration takes effect automatically. At the next Product-defined attempt to start new licensed work, or the next scheduled check-in that the signed decision permits, the Product contacts the license service. If the account is again in good standing, Provider returns a newer signed grant and full function resumes without a support ticket, approval, or manual reissue. Opening, reading, auditing, exporting, or verifying existing records never requires that contact. The retention lease in Section 21B.1 resumes extending with each payment. The rule is the same in both directions and no human judgement is applied to either.

21B.2A Downgrades

A downgrade shortens the retention window to the one published for the new plan. Evidence that falls outside the shorter window stops being covered by custody, but it is not removed the moment the change takes effect.

Provider gives Client an export window before that evidence leaves custody, on the same footing as the export period an account closure receives, so that a plan change never causes data loss on the day it is made. Client is responsible for exporting within that window. Where the storage expiry date under Section 21B.1 falls later, nothing is deleted before it passes.

Downgrading is not a way to keep a long retention tail at a shorter tier's price. Once the export window closes, evidence outside the new window is no longer retained, and Provider has no obligation to restore it if Client upgrades again later.

21B.2B Cancellation and the End of a Lease

Cancelling does not switch anything off. Client has paid for a period and the lease covers that period, so the Products keep working normally until it ends. A Client who cancels on day fifteen of a thirty-day period keeps full function for the remaining fifteen

days. Provider does not shorten a lease that has been paid for, and the Product is not told that a cancellation happened: it holds the lease it was granted and runs.

A lease can end for three reasons: Client cancelled, the account closed under Section 21B.2, or a plan was not renewed under Section 44. In each case, once the lease ends and is not renewed, the Product stops doing new work and keeps doing read-only work. This is the same state Section 21B.2 describes. bug creates no new records or reports and continues to open, read, and audit records already created. witness accepts no new runs, evidence, or timestamping and continues to verify evidence already held. peachfuzz stops, because it is a continuous service with nothing to read back.

That read-only capability is a licence that expressly survives termination for the purposes of Section 47, and it is not time-limited. Client does not lose the ability to read, audit, and verify what it already produced merely because it stopped subscribing. What Client made is Client's, and the Product goes on letting Client read it.

Nothing else survives with it. The read-only licence carries no support, no updates, no new features, no service level, no custody, and no entitlement to install the Product on additional devices or to register devices beyond what the last paid period covered. It remains subject to Sections 30 and 30B in full. Doing new work again requires a current subscription.

21B.3 Export, Deletion, and Responsibility

Exporting data is Client's responsibility, and Client has the whole period described above in which to do it. Provider has no obligation, during a lapse, to accept new data, extend retention, provide support, perform custom or bespoke exports, preserve convenience features, or keep nonessential services running.

Once deleted, data is gone from active systems, indexes, backups, and storage on Provider's ordinary cycles, unless a paid-up archive, legal hold, court order, law, unexpired storage expiry date, or signed Order requires Provider to keep it.

Provider is not liable for loss, deletion, expiry, inaccessibility, or non-extension of data caused by nonpayment, cancellation, lapse, account closure, plan expiry, abandonment, an inaccurate billing

contact, or failure to export during the period available. Client received notice, retained read access to what it already had, and had months to export.

21B.4 Cancellation Ends Custody

A retention term describes how long Provider will hold data while Client keeps paying to have it held. It is not a deposit, an escrow, a prepayment for future storage, an insurance policy against a future dispute, or a guarantee that survives the account.

This is the case most likely to be misunderstood, so it is stated plainly rather than left to be inferred. A Client that seals evidence with witness, releases its software, cancels its account, and returns two years later expecting Provider to produce that evidence will find that it no longer exists. Cancellation started the wind-down described in Section 21B.2. The notices were sent to the contact on file. The storage expiry passed. The data was deleted. Provider is not an archive of last resort and does not hold data for a Client who has stopped paying to have it held. Buying a ten-year term and paying for two months buys two months of custody plus the remaining lease window, not ten years.

After an account has closed, Provider has no obligation to retain, restore, reconstruct, re-create, or re-issue any data, evidence, seal, certificate, report, or record; to produce a copy of anything for Client, Client's counsel, an auditor, a regulator, a court, an insurer, an opposing party, or anyone else; to confirm, certify, attest to, or vouch for anything Client previously held; or to provide an affidavit, declaration, statement, expert opinion, or testimony about it. Paying an overdue amount after deletion restores nothing, because there is nothing left to restore.

21B.5 Self-Hosted and On-Premises Deployment

Some Clients want the software under their own control rather than the custody service around it. That is available where an Order expressly provides for it, and it is a different transaction from the one the rest of this Section describes.

Self-hosted deployment is licensed and priced separately. The fees for it are stated in the Order, are in addition to any other fees, and are payable whether or not Client also uses any hosted service. A self-hosted licence is limited to the instances, environments, Organization License, Registered Devices, and term

the Order states, is for Client's own internal business use, and remains subject to Sections 30 and 30B in full, including the prohibitions on hosting the Products for third parties, reselling them, and circumventing licence controls.

Provider holds nothing in a self-hosted deployment, and nothing in this Section 21B applies to it. There is no retention lease, no storage expiry date set by Provider, no payment ladder affecting stored data, and no deletion by Provider, because Provider has no copy and no access. Client is responsible for its own storage, retention, retention locks, immutability, backups, disaster recovery, access control, key management, residency, availability, monitoring, and integrity.

What Client trades away is independence, and it is worth stating plainly rather than discovering during an audit. Evidence held by the party that produced it is not evidence held by anyone else. The reason Provider's custody has value to an auditor, a customer, a regulator, or a court is that the records sit with a party that has no stake in what they say. A self-hosted deployment removes that party. Provider makes no representation that self-held records will satisfy an auditor, assessor, customer, insurer, regulator, or court that requires evidence to be held independently, and Client accepts that trade knowingly in exchange for control.

Provider cannot produce, restore, verify the custody of, or give any declaration about data it has never held. Section 21B.6 is not available for self-hosted deployments, and neither is any statement by Provider about how Client stored, protected, or handled its own records.

Where a self-hosted deployment still calls Provider's timestamping or licence services, those calls remain governed by this Agreement and by the applicable fees. Where a deployment is configured not to call them, Client arranges and pays for its own trust services, and Provider is not responsible for them, for their availability, or for the acceptability of anything they produce.

On expiry or termination of a self-hosted licence, Client must stop using the software under Section 47. Records Client has generated and holds remain Client's own; Provider claims no rights in them and takes on no obligation in respect of them.

21B.6 Custodian's Declaration

Where an Order or the published plan includes it, and only while the account is active and in good standing, Provider will on request prepare a written custodian's declaration in respect of evidence Provider holds for Client. It is the baseline of what Provider provides by way of speaking to a record, on every Product and every plan that includes it, and the same terms apply in each case. Section 21B.7 states the separately ordered engagements that go beyond a document. The declaration describes Provider's own process: how the record was received and stored, that it was held under a retention lock and for what period, what the system recorded about it, and what Provider's records show. It is a statement about Provider's custody, made by the person who operates it.

Provider charges for each declaration at the rate stated in the Order or, if none is stated, at Provider's then-current professional services rate with a minimum of one hour.

What a declaration is not, stated so that no one buys it expecting something else: by itself it is not an appearance before a court, tribunal, arbitrator, regulator, or auditor, and it is not testimony, cross-examination, discovery, or deposition. Those are separate engagements under Section 21B.7, separately ordered and separately priced, and a declaration does not include one. A declaration is also not an expert opinion on Client's software, controls, compliance posture, or dispute, and not an opinion on whether anything Client did was correct, adequate, or lawful. Section 10 continues to apply. Provider does not guarantee that any court, auditor, regulator, insurer, or other third party will accept or give any weight to a declaration.

Where Provider is compelled by valid legal process to do more than this, Section 48A applies, including Client's obligation to reimburse Provider's costs and time.

This Section applies only while the account is active. Once an account has closed, Section 21B.4 governs and Provider owes nothing, including no declaration about evidence it no longer holds.

Where Provider is compelled by valid legal process to respond in respect of a former Client, Section 48A applies, including Client's obligation to reimburse Provider's costs, and Provider's response is limited to whatever Provider still holds at that time.

What Client keeps is what Client exported. Evidence exported from witness is built to stand on its own: it carries the hash, the timestamp token, the certificate chain, and the verification metadata needed for anyone to check it independently, without Provider's participation and without Provider continuing to exist. That is the point of the design, and it is why exporting before cancellation is the whole of Client's protection. As Section 9 states, Provider does not guarantee that any auditor, court, regulator, customer, or other third party will accept exported evidence.

Provider's own operational records are not Client's archive. Provider may keep server logs, timestamp request and response records, billing records, and security records for its own operational, audit, legal, and compliance purposes, for the periods described in the Privacy Policy. Those records exist for Provider's purposes, are not a copy of Client's evidence, are not maintained for Client's benefit, and give Client no right to demand production, reconstruction, or certification of anything after custody has ended.

If Client wants custody that outlives its subscription, that is a different purchase: a paid-up archive under a signed Order, priced for the term and paid for in advance.

21B.7 Explaining the Record: Calls, Attendance, and Testimony

A declaration under Section 21B.6 is a document. Some Clients need a person as well, and where the published plan or an Order includes it Provider offers that separately. This Section states what is available, what it costs, and what it is not, so that nobody buys it expecting something else.

Two engagements are available:

- A call. Provider will attend a telephone or video call with Client's auditor, assessor, insurer, counsel, customer, or reviewer, to explain what Provider holds, how it was received and stored, and how the record is verified.
- An appearance. Provider will attend before a court, tribunal, arbitrator, or regulator to give evidence about the same matters.

Both are separately ordered and separately priced, at the rate stated in the Order or, if none is stated, at Provider's then-current professional services rate, with a minimum of one hour for a call. Both are scheduled by agreement and are subject to Provider's availability, including in respect of any date fixed by someone other than the Parties. Neither is included in a subscription fee. A plan that lists the engagement buys Client the right to order it, not an appearance on demand.

What Provider will speak to is Provider's own custody: that the record was received, when it was received, how it was stored, that it was held under a retention lock and for what period, what Provider's systems recorded about it, and how the record is verified. That is the same subject matter as a declaration under Section 21B.6, spoken rather than written.

What Provider will not speak to, on any engagement and at any price: whether Client's software was correct, secure, or fit for purpose; whether Client's controls were adequately designed or operated; whether Client's tests, evidence, or engineering judgement were sufficient; whether Client complied with any law, standard, framework, certification, or contract; or whether anything Client did was reasonable, adequate, or lawful. Provider is a custodian, not an expert witness on Client's engineering or compliance, and Section 10 applies in full. Provider will say so in advance and will decline a question outside that scope.

Provider does not guarantee that any court, tribunal, arbitrator, regulator, auditor, insurer, or other third party will qualify Provider to give evidence, admit that evidence, or give it any weight. Whether a tribunal accepts a witness is the tribunal's decision, and no vendor can promise it.

This Section applies only while the account is active and in good standing, and only in respect of evidence Provider then holds. Once an account has closed, Section 21B.4 governs and Provider owes nothing, including no call and no appearance. Where Provider is compelled by valid legal process rather than engaged by Client, Section 48A applies instead, including Client's obligation to reimburse Provider's costs and time.

Provider may decline an engagement, including where it would conflict with an obligation owed to another client, where the scope sought exceeds this Section, or where Provider's availability does not permit it. Where Provider declines an engagement for which

Client has already paid and which Provider has not performed, Provider will return that fee. This is an express exception to Section 19, and it is the only one this Section creates.

22. Taxes and Withholding

Fees are exclusive of applicable taxes unless stated otherwise. Client must pay all HST, GST, PST, QST, sales tax, use tax, VAT, withholding tax, duties, levies, and similar charges arising from the Agreement, except taxes based on Provider's net income.

If Client is required by law to withhold an amount, Client must gross up the payment so Provider receives the full amount invoiced, unless the Parties agree otherwise in writing.

23. Hosting, Domains, SSL/TLS, and Third-Party Platforms

Hosting, domains, SSL/TLS certificates, email, analytics, payment processors, cloud infrastructure, CI systems, source control systems, registrars, marketplaces, and other third-party platforms are subject to third-party terms, fees, availability, security, rate limits, policies, outages, and changes.

Provider is not responsible for third-party outages, policy changes, price changes, security incidents, account suspensions, API changes, domain registry failures, DNS propagation delays, email deliverability failures, marketplace rejections, search engine changes, payment processor holds, or platform conduct outside Provider's control.

Client owns its domain name unless an Order states otherwise. Client must keep registration, billing, access, and ownership information current. If Provider manages a domain, Client must provide timely approvals and payment. Provider is not responsible for domain loss, expiry, suspension, or transfer delay caused by Client delay, inaccurate account information, third-party registrar issues, or nonpayment.

24. Maintenance and Support

Maintenance and support are provided only if included in an Order or active plan. Unless an Order states otherwise:

- Support is provided during Provider's normal business hours.

- Response times are targets, not guaranteed resolution times.
- Support excludes new features, redesigns, third-party outages, emergency response, incident response, security remediation, compliance remediation, data recovery, client-caused issues, custom training, and work outside the supported version.
- Unused support time, maintenance time, retainers, and subscription periods do not roll over.

Provider may refuse support for unpaid accounts, unsupported versions, modified code, insecure configurations, missing access, unlawful use, abusive conduct, or systems outside the agreed support scope.

24A. Custody Durability Commitment

Where a published plan states that it includes a service level, this Section is that service level, and it is the only one Provider offers on any Product. It is a commitment about the record rather than about availability. Provider makes no uptime, latency, throughput, or response-time commitment anywhere in this Agreement, and Sections 11, 24, and 37 continue to apply to all of those in full.

This Section is a commitment for the purposes of Section 5A. Nothing on Provider's website, in a proposal, in a demo, or in a support channel is a service level unless it is stated here or in a signed Order.

What is committed. For each Custody Artifact and each Cloud Evidence object Provider has accepted and issued a receipt for, and for as long as the applicable Retention Lease runs under Section 21B, Provider commits that:

- the object remains retrievable by Client through the available export method, subject to authentication and to the security controls in this Agreement;
- the object is returned with the same bytes Provider accepted, so that it verifies exactly as it did on acceptance; and
- the object is held under a storage expiry that cannot be brought forward, by Provider or by anyone else, before the date Section 21B.1 sets.

How a failure is measured. A failure means a request by Client, through the available export method, for an object within its Retention Lease, which Provider does not fulfil within five business days of the request, or which Provider returns in a state that no longer verifies against the receipt Provider issued for it.

What is excluded. This commitment does not apply where the object was never accepted and receipted; where the Retention Lease has ended under Section 21B for any reason, including cancellation, non-renewal, lapse, downgrade, or account closure; where retrieval is delayed or refused under Section 21, Section 30A, or Section 48A; where the failure is caused by Client's account state, credentials, configuration, or instructions; where deletion is required by law, court order, or Client's own request; or during a force majeure event under Section 51.

The remedy. Where Provider fails this commitment, Client's exclusive remedy is a credit of one month's fees for the affected plan for each month in which a failure occurs, up to three months' fees in aggregate in any twelve-month period, applied to Client's next invoice. Client must claim the credit in writing within thirty days after the failure. This is an express exception to Section 19 and it is the only credit this Agreement provides. It does not make any fee refundable, and Section 39 continues to cap Provider's liability for everything beyond this credit.

25. Security

Provider will use commercially reasonable security practices appropriate to the scope and fees of the Order. Security practices may include access controls, least-privilege access, secrets handling, dependency review, secure development practices, logging, or testing as Provider determines appropriate.

Four controls are not left to Provider's discretion, because Provider sells them. For every Custody Artifact and every Cloud Evidence object Provider holds, Provider will encrypt it in transit and encrypt it at rest; hold it in storage private to Client's tenant and not readable by another customer; store it content-addressed and create-only, so that an accepted object cannot be silently replaced; and hold it under the storage expiry described in Section 21B.1 so that it cannot be deleted before that date passes. Those

four are commitments rather than examples. Provider will not remove one from a Product a Client is already paying for, and the authority in Section 35B does not extend to removing them.

No system is perfectly secure. Provider does not guarantee prevention of unauthorized access, data loss, malware, ransomware, credential compromise, supply-chain compromise, third-party breach, insider threat, zero-day exploit, misconfiguration, phishing, denial of service, or vulnerability.

Client is responsible for its own security program, access control, employee training, endpoint security, identity provider, backups, production monitoring, vulnerability management, incident response, legal notices, breach notices, and compliance obligations.

25A. Shared Responsibility for Identity, Access, and Configuration

Security, identity, access control, and configuration are shared-responsibility areas. Unless an Order expressly assigns a specific responsibility to Provider, Client is responsible for identity-provider configuration, SSO, MFA, OAuth apps, API keys, secrets, webhooks, role design, permission assignments, privileged users, employee onboarding and offboarding, service accounts, session settings, password-reset flows, account recovery, access reviews, audit-log review, production authorization logic, and downstream use of Provider deliverables.

Provider may recommend or implement technical controls, but implementation support does not transfer ownership of Client's access governance, account security, or production authorization model unless a signed Order expressly states otherwise.

25B. Security Incident Notification

If Provider confirms a security incident that has resulted in unauthorized access to, unauthorized disclosure of, or loss of Client Materials or Client personal information under Provider's control, Provider will notify Client without undue delay and in any event within seventy-two hours after confirming the incident.

The notice will state what Provider knows at the time, including the nature of the incident, the categories of information involved, the systems or Products affected, the period concerned if known,

what Provider has done in response, and what Client may need to do. Provider will update Client as the investigation develops and will correct earlier information that turns out to be wrong.

Notice will be sent to Client's security or notice contact, or if none is designated, to the billing or account contact on file. Client is responsible under Section 7 for keeping that contact accurate and current, and a notice sent to the contact on file is effective even if Client has not maintained it.

Provider will cooperate reasonably with Client's own investigation and with Client's notification obligations to its users, customers, employees, insurers, and regulators. Cooperation that goes beyond Provider's own incident response, including custom forensic work, evidence production, questionnaire completion, or support for Client's regulator interactions, is billable at Provider's then-current rates unless a signed Order states otherwise.

An initial or interim notice is given so Client can act quickly. It is not an admission of fault, liability, breach of this Agreement, or breach of any law by Provider, and it does not extend, restart, or waive any limitation period, cap, or defence.

This section states Provider's notification obligation to Client. It does not change Provider's separate obligations under the Privacy Policy and applicable Canadian privacy law, including Provider's obligation under PIPEDA to report a breach of security safeguards to the Office of the Privacy Commissioner of Canada and to notify affected individuals where the breach creates a real risk of significant harm. Client remains responsible under Sections 25 and 25A for incidents in Client's own systems, accounts, credentials, identity providers, configurations, and vendor relationships, and for its own regulatory notifications.

26. Regulated Data and Data Processing

Client must not provide Regulated Data unless the applicable Order expressly permits it and the Parties have signed any required data processing agreement, business associate agreement, security addendum, or regulated-data addendum.

Client is responsible for determining whether PIPEDA, PHIPA, GDPR, UK GDPR, CCPA/CPRA, HIPAA, GLBA, FERPA, PCI DSS, export controls, data residency rules, breach notification rules,

sector-specific laws, or other privacy/security requirements apply to Client Materials or Client's use of the Services or Products.

Client represents that it has all required rights, notices, consents, permissions, lawful bases, contracts, and authorizations for Provider to process Client Materials as necessary to provide the Services and Products.

Provider may process Client Materials to provide, secure, troubleshoot, support, improve, and document the Services and Products, subject to confidentiality obligations and any signed data processing terms.

26A. Territorial Scope of the Offering

Provider is a Canadian company operating from Ontario, Canada. The Services, Products, and Off Grid Properties are offered to businesses in Canada and the United States. Provider does not offer, market, target, advertise, solicit, price, localize, translate, or make the Services or Products available to individuals or organizations in the European Economic Area, the United Kingdom, or Switzerland, does not accept EEA, UK, or Swiss currencies, and does not monitor the behaviour of individuals located in those territories. Any incidental accessibility of a public web page from those territories is not an offering, is not targeting, and does not indicate an intention to serve those markets. Section 2B states the terms on which Provider serves business clients established in Quebec.

Client must not submit, upload, route, transmit, store, process, or otherwise cause Provider to receive personal data of individuals located in the European Economic Area, the United Kingdom, or Switzerland, and must not use the Services or Products to monitor the behaviour of such individuals, unless Provider has agreed to that use in a signed order and a signed data processing addendum that states the applicable terms, fees, safeguards, and transfer mechanism. Provider offers no such addendum by default and may decline to enter into one.

Provider makes no representation, warranty, or commitment that the Services, Products, or Off Grid Properties satisfy the General Data Protection Regulation, the UK GDPR, the Swiss Federal Act on Data Protection, or any other law of those territories, and Provider undertakes no obligation of a controller, processor, or

representative under those laws. Provider's privacy obligations are those stated in the Privacy Policy and in applicable Canadian law, including PIPEDA and applicable provincial privacy legislation.

If Client breaches this Section 26A, Client is solely responsible for the consequences, Provider may suspend or terminate the affected Services, Products, or account under Sections 30A and 46, and Client will indemnify Provider under Section 41 for all resulting claims, investigations, regulatory proceedings, fines, penalties, and costs.

Nothing in this Section 26A limits any Canadian privacy, security, or breach-notification obligation that applies to Provider, or any obligation Provider expressly accepts in a signed Order.

27. Confidentiality

Each Party will protect the other Party's Confidential Information using reasonable care and at least the same care it uses for its own similar information.

The receiving Party may use Confidential Information only to perform or receive benefits under this Agreement. The receiving Party may disclose Confidential Information to employees, contractors, advisors, auditors, lawyers, accountants, insurers, hosting providers, subprocessors, and financing sources who need to know it and are bound by confidentiality obligations or professional duties.

Confidentiality obligations do not apply to information that:

- Is or becomes public without breach.
- Was already known without confidentiality restriction.
- Is independently developed without use of the disclosing Party's Confidential Information.
- Is received from a third party without known confidentiality breach.
- Must be disclosed by law, subpoena, regulator, court, arbitrator, or stock exchange rule, provided the receiving Party gives notice when legally allowed.

Confidentiality obligations survive for five years after termination. Trade secrets, credentials, source code, security information, audit evidence, and regulated data remain protected for as long as they remain non-public and legally protectable.

28. Client Materials

Client retains ownership of Client Materials. Client grants Provider a non-exclusive, worldwide, royalty-free license to use, copy, modify, process, transmit, host, display, test, and create derivative works from Client Materials as necessary to provide the Services and Products.

Client represents and warrants that Client Materials do not infringe, misappropriate, violate privacy rights, violate publicity rights, violate confidentiality obligations, violate laws, contain unlawful content, contain malicious code, or require Provider to violate third-party terms.

Provider may remove, refuse, or suspend work involving Client Materials that Provider reasonably believes are unlawful, infringing, unsafe, misleading, abusive, security-sensitive beyond the agreed scope, or likely to create liability.

29. Intellectual Property Ownership

Subject to full payment of all amounts due, Client owns custom Deliverables expressly created for Client under a custom Services Order, excluding Provider Background IP, third-party materials, open-source software, Product software, generic components, know-how, templates, methodologies, and tools.

Provider retains all rights, title, and interest in Provider Background IP. No rights transfer by implication, estoppel, access, delivery, payment, or use.

Until Provider has been paid in full, Client owns nothing and licenses nothing. Every design, layout, wireframe, prototype, mockup, staging build, demo environment, screen share, source file, and other Deliverable or work in progress remains Provider's property. Client has no licence to use, publish, deploy, launch, copy, adapt, or reproduce any of it, and no right to have it copied, adapted, recreated, or rebuilt by anyone else. Access to a demo, a staging site, or a screen share is permission to look at the work, not permission to take it.

While any amount is outstanding, Client will not use, and will not permit any employee, contractor, agency, developer, designer, offshore team, or other third party to use, copy, trace, adapt, re-implement, or recreate any Deliverable or work in progress, in whole or in substantial part, whether from delivered files, a

repository, a staging or demo environment, a screen share, a recording, a screenshot, or a description of what Client saw. Showing the work to a third party who then reproduces it is a breach of this section by Client, and the fact that another party did the copying does not excuse it.

If Client breaches this section, the full fees stated in the Order remain due and payable in full and are not reduced, offset, or excused by the breach; ownership of the Deliverables does not transfer and will not transfer while the breach continues; Provider may pursue the reproduction as copyright infringement against Client and any party acting for or with Client; and Provider may seek immediate injunctive relief in court under Section 57 instead of proceeding under Section 54. These remedies are cumulative and are in addition to every other remedy available to Provider. For clarity, none of the caps or exclusions in Section 39 limit Client's obligations under this section.

To the extent Provider Background IP is embedded in a custom Deliverable and necessary for Client to use that Deliverable, Provider grants Client a non-exclusive, non-transferable, non-sublicensable, perpetual license to use that embedded Provider Background IP solely as part of the Deliverable for Client's internal business purposes, subject to payment and this Agreement.

Products are licensed, not sold. Client receives only the license rights expressly stated in the applicable Order or Product terms.

30. Product License Restrictions

Unless an Order expressly permits otherwise, Client must not:

- Copy, resell, sublicense, distribute, rent, lease, timeshare, or commercially host the Products for third parties.
- Reverse engineer, decompile, disassemble, scrape, or attempt to derive source code, non-public APIs, models, or internal logic.
- Remove proprietary notices.
- Circumvent license keys, usage limits, metering, access controls, rate limits, or security controls.
- Use Products to build a competing product or service.

- Use Products for unlawful surveillance, credential theft, spam, malware, exploitation, fraud, harassment, deception, or unauthorized testing.
- Use Products in life-safety, weapons, critical infrastructure, emergency services, nuclear, aviation, medical-device, or other high-risk systems where failure could cause death, bodily injury, severe property damage, or severe environmental harm.
- Permit third parties to access Products except authorized users working for Client's internal business purposes.

For clarity, Client may not resell, redistribute, sublicense, rent, lease, lend, host, or otherwise make bug, witness, or peachfuzz, or access to them, available to any third party, and may not act as a reseller, distributor, or marketplace for bug, witness, or peachfuzz, unless a signed Order or a separate written reseller agreement with Provider expressly permits it. Every Organization License and Registered Device activation is for Client's own internal business use only. Registering a device that belongs to, or is operated by, any person or entity other than Client and its authorized users is prohibited whether or not Client's plan caps the number of Registered Devices, and an uncapped plan is not permission to license anyone else's machines.

Provider may suspend or terminate access for suspected license breach, security risk, unlawful use, nonpayment, or use that threatens Provider, other customers, or third parties.

30A. Acceptable Use, Abuse Monitoring, and Emergency Suspension

Client and its authorized users must comply with Provider's acceptable use rules, security instructions, documentation, and reasonable operational limits. Provider may investigate suspected abuse, misuse, unlawful activity, security risk, license breach, platform risk, excessive usage, spam, malware, scraping, credential abuse, denial-of-service activity, unauthorized access, or violation of third-party platform rules.

Provider may immediately suspend or restrict any Service, Product, account, domain, integration, API token, deployment, repository access, hosting environment, feature, or user if Provider reasonably believes suspension is needed to protect

Provider, Client, other customers, end users, infrastructure, third-party platforms, data, legal compliance, security, reputation, or service integrity.

Provider may remove, disable, quarantine, limit, or refuse content, code, integrations, traffic, accounts, features, or configurations that Provider reasonably believes are unlawful, infringing, abusive, unsafe, misleading, security-sensitive, technically harmful, or likely to create liability. Provider is not liable for losses arising from good-faith suspension, restriction, removal, investigation, or refusal under this section.

Client is responsible for all activity under Client accounts, credentials, tokens, domains, repositories, payment methods, users, administrators, and environments, whether or not Client authorized or knew about the activity, except to the extent caused by Provider's willful misconduct.

30B. Reverse Engineering and Technological Protection Measures

The bug, witness, and peachfuzz binaries, together with their license keys, signatures, Product Leases, device registrations and activation checks, metering, and update mechanisms, are technological protection measures that control access to and use of Provider's proprietary software. Except to the minimum extent a non-waivable law expressly permits, Client and its users must not reverse engineer, decompile, disassemble, deobfuscate, or otherwise attempt to derive the source code, internal logic, non-public interfaces, or cryptographic material of any bug, witness, peachfuzz, or other Provider binary, and must not circumvent, disable, bypass, or tamper with any license key, signature, Product Lease, device registration, activation check, metering, or other technological protection measure.

These restrictions are contractual and are also protected by law, including the technological protection measure provisions of the Copyright Act (Canada) and, for United States users, the anti-circumvention provisions of the Digital Millennium Copyright Act. Nothing in this section prevents Client from exercising a right that cannot be waived by contract, such as a statutory interoperability, repair, maintenance, or security-research exception, strictly to the extent that right applies and cannot lawfully be excluded.

31. Open Source and Third-Party Materials

Deliverables and Products may include open-source software or third-party materials. Those materials are governed by their own licenses and terms. Nothing in this Agreement limits rights Client may have under applicable open-source licenses.

Provider is not responsible for Client's failure to comply with third-party licenses, third-party platform terms, export restrictions, attribution requirements, or procurement requirements unless a signed Order expressly assigns that responsibility to Provider.

32. Feedback

Client may provide ideas, suggestions, bug reports, feature requests, workflows, tests, evidence formats, or other feedback. Provider may use feedback without restriction, payment, attribution, or obligation, provided Provider does not disclose Client Confidential Information in violation of this Agreement.

33. Portfolio and Publicity

Provider may identify Client as a customer and may display non-confidential project summaries, screenshots, names, logos, links, and case studies in Provider's portfolio, website, sales materials, proposals, and investor materials unless Client opts out in writing before publication.

Provider will not knowingly publish Client Confidential Information, security-sensitive implementation details, non-public audit evidence, credentials, private repositories, or regulated data.

34. Marketing, Email, and Communications Compliance

If Provider builds or supports marketing websites, email flows, lead capture, analytics, advertising, SMS, newsletters, or outreach tooling, Client remains responsible for compliance with applicable marketing, privacy, anti-spam, consumer protection, platform, and advertising laws, including CASL in Canada and CAN-SPAM in the United States.

Client is responsible for consent records, unsubscribe handling, lawful contact lists, truthful claims, privacy notices, cookie notices, advertising substantiation, accessibility obligations, and

sector-specific marketing restrictions unless an Order expressly states otherwise.

34A. Client Sites, Storefronts, End Users, and Customer Policies

If Provider builds, hosts, supports, integrates, or supplies tooling for any Client website, application, ecommerce store, booking flow, subscription flow, member area, payment flow, community, form, portal, API, or public-facing workflow, Client remains solely responsible for Client's customers, visitors, users, members, buyers, subscribers, vendors, contractors, and other end users.

Client is solely responsible for products and services sold or promoted through Client systems, product claims, pricing, taxes, duties, shipping, fulfillment, refunds, returns, warranties, chargebacks, customer support, consumer notices, age gates, accessibility, marketplace rules, payment processor rules, professional licensing, regulated goods, and industry-specific restrictions.

Client must publish and maintain legally adequate terms of service, privacy policy, refund policy, cookie notice, accessibility notice, customer support process, and any other notices required for Client's business, industry, customers, geography, data, and sales model unless an Order expressly assigns drafting responsibility to Provider.

Provider does not provide legal advice to Client or Client end users and is not responsible for claims by, on behalf of, or against Client end users, including claims relating to Client's products, services, sites, stores, content, data collection, cookies, pixels, payments, refunds, taxes, fulfillment, or customer support.

34B. Pixels, Cookies, Analytics, Tracking, and Customer Consent

Client is responsible for obtaining and recording all required consents and providing all required notices for cookies, pixels, analytics, session replay, advertising tags, conversion APIs, email tracking, SMS tracking, CRM tracking, payment tracking, and similar technologies used on or through Client systems.

Provider may implement tracking, analytics, consent, or privacy tooling only as a technical service. Provider does not warrant that any banner, policy, preference center, tag manager, consent mode, analytics configuration, or tracking setup satisfies any law or platform rule unless a signed Order expressly states the exact legal standard and acceptance criteria.

34C. Off Grid Software Electronic Messages and Software Installation

Client consents to receive transactional, administrative, security, billing, support, and service electronic messages from Provider in connection with the Services, Products, and Off Grid Properties. Provider may also send commercial electronic messages, such as product news and offers, and will identify itself, identify on whose behalf each message is sent where applicable, and provide a working unsubscribe mechanism in each such message, consistent with Canada's anti-spam legislation. Client may withdraw consent to commercial electronic messages at any time using that mechanism, without affecting transactional or service messages Provider needs to send.

By downloading, installing, activating, registering a device for, or updating bug, witness, peachfuzz, or any Off Grid Software binary, agent, daemon, or update, Client consents to that installation and to the device registration, periodic updates, and license check-ins described in Section 7A, the applicable Product terms, and the Privacy Policy. Client is responsible for obtaining any consent its own users, employees, or contractors require before Client installs a Provider binary on their devices.

35. Artificial Intelligence, Agents, and Automation

Provider may use software agents, automation, AI-assisted tools, compilers, test runners, linters, static analysis tools, code generators, documentation generators, or other tools to provide Services and Products.

Client acknowledges that agentic and automated outputs may be incomplete, outdated, wrong, insecure, non-compliant, or unsuitable without human review. Provider does not guarantee that AI-assisted or agentic outputs will be correct, complete, non-infringing, secure, or compliant.

Client must review all generated code, tests, evidence, policies, reports, and recommendations before relying on them.

35A. Usage Data, Telemetry, Aggregated Data, and Public Fields

Provider may collect and use technical, diagnostic, security, usage, performance, billing, abuse-prevention, and operational data about the Services and Products to provide, secure, debug, support, bill, improve, and plan the Services and Products.

Provider may create and use aggregated, de-identified, anonymized, or statistical data derived from use of the Services and Products for analytics, benchmarking, security, product improvement, planning, and marketing, provided it does not identify Client or disclose Client Confidential Information.

Client must not place secrets, credentials, tokens, private keys, personal information, regulated data, sensitive security details, or confidential information in public fields, account names, project names, repository names, branch names, commit messages, ticket titles, URLs, DNS records, metadata, logs intended for public sharing, or support channels not designated for confidential exchange. Provider is not responsible for exposure caused by Client placing sensitive information in public, shared, or unsupported fields.

Unless an Order expressly permits otherwise, Provider will not train public AI models on Client Confidential Information. Provider may use Client feedback, de-identified usage patterns, telemetry, and non-confidential suggestions to improve Provider products and services, subject to this Agreement.

35B. APIs, Quotas, Feature Changes, Benchmarking, and Service Evolution

Provider may set and enforce quotas, rate limits, storage limits, registered-device limits permitted by Section 7A, usage limits, fair-use limits, API limits, file-size limits, build limits, retention limits, and other technical or commercial controls. Usage above included limits may be billed as overage, throttled, rejected, queued, or require an upgraded plan, but a limit does not silently change an Organization License into a per-user, per-repository, per-project, per-core, or per-device price meter.

Provider may modify, discontinue, suspend, replace, deprecate, or make backwards-incompatible changes to features, APIs, integrations, models, agents, templates, documentation, SDKs, CLIs, hosting configurations, or third-party dependencies when Provider reasonably determines the change is needed for security, legal compliance, service integrity, product improvement, commercial feasibility, vendor change, third-party platform change, or technical maintenance.

That authority does not override Sections 7A, 7B, 19A, 21B, or 44. Provider may change the catalog and legal terms for future Orders, but may not use an API, feature, vendor, or implementation change to silently alter an active Client's Organization License meter, paid Product Lease authority, trial already in progress, permitted-data ceiling, custody window, accepted-artifact integrity, signed receipt, retention lock, export window, or held rate. A change to one of those commitments requires the authority the controlling Section itself permits.

Provider will use commercially reasonable efforts to avoid unnecessary disruption to generally available paid features, but Client acknowledges that security, law, vendor change, abuse prevention, infrastructure integrity, and commercial feasibility may require changes with limited or no advance notice.

Client may not publicly disclose performance tests, benchmark results, security test results, vulnerability details, availability measurements, competitive comparisons, or technical reviews of Products or hosted Services without Provider's prior written consent, except where prohibited by law. This does not restrict Client from making confidential disclosures to its lawyers, auditors, regulators, insurers, investors, or security advisors under appropriate confidentiality obligations.

35C. AI Output, Similarity, Accuracy, and Human Review

AI, agentic, or automated outputs may be inaccurate, incomplete, misleading, outdated, biased, unsafe, non-unique, non-copyrightable, or similar to outputs generated for others. Client must independently review outputs before using them in production, audits, legal positions, customer communications, marketing campaigns, regulated decisions, or security decisions.

Client is responsible for notices, disclosures, human review, end-user instructions, and independent verification needed for Client's use case. Client must not submit health information, payment card data, government identifiers, children's data, export-controlled data, or other regulated data to AI or automation features unless the applicable Order and required addendum expressly permit it.

Client may not use Products or outputs to train competing foundation models, reverse engineer model behavior, extract hidden system prompts, bypass safety systems, or violate third-party AI, API, or platform terms.

35D. Logs, Telemetry, Error Reports, and Sensitive Data

Unless an Order expressly permits otherwise, Client must not place sensitive personal information, PHI, payment card data, financial account numbers, government identifiers, trade secrets, production secrets, private keys, access tokens, customer passwords, or regulated data in logs, traces, crash reports, error messages, support tickets, telemetry fields, analytics events, issue titles, debugging payloads, or the fuzzing seed corpora from which Section 9A.1 uploads are derived.

Provider's side of the same subject is stated here, because a prohibition addressed only to Client says nothing about what Provider does. Provider collects diagnostic, crash, and error information about Provider's own binaries and Provider's own services, because a product that cannot report its own failures is a product Provider cannot fix. What Provider wants from that channel is Provider's own defects. Provider takes reasonable measures to keep customer-controlled content out of it, and the strongest of those measures is structural rather than a promise of restraint: as Section 7A states, Product wire bodies are composed of named identities, closed enums, bounded numbers and durations, typed instants, hashes, and signatures, and contain no free-form payload strings, generic metadata maps, untyped extension objects, opaque telemetry blobs, or catch-all byte fields. A payload with nowhere to put a secret does not carry one by accident. Reasonable measures are not a guarantee, and Provider commits to the control rather than to an outcome Provider does not fully govern. Provider does not use diagnostic data to profile Client's individual developers, and Section 35A governs its use.

Monitoring, logging, tracing, alerting, evidence collection, linting, scanning, and error-reporting tools are operational aids only. Provider does not guarantee that they will detect, identify, prevent, preserve, classify, prioritize, or correct every bug, incident, vulnerability, outage, control failure, evidence gap, or compliance issue.

Storage limits, sampling, retention schedules, account downgrades, plan changes, deletions, export limits, and suspension may result in loss of logs, telemetry, evidence, alerts, history, or product data, and Provider is not liable for loss caused by Client configuration, nonpayment, plan limits, or third-party platform limits.

36. Warranty for Custom Services

For custom Services, Provider warrants that it will perform the Services in a professional and workmanlike manner. Client's exclusive remedy for breach of this limited warranty is re-performance of the nonconforming Services or, if Provider determines re-performance is commercially unreasonable, a refund of the fees paid for the specific nonconforming Services.

Client must report warranty claims in writing within thirty days after delivery. The warranty does not apply to issues caused by Client Materials, Client changes, third-party services, unsupported environments, misuse, unauthorized modifications, nonpayment, security incidents outside Provider's control, open-source components, production data, changed requirements, changed laws, changed third-party APIs, or systems outside the agreed scope.

37. Product Warranty Disclaimer

Products, hosted services, license keys, documentation, templates, examples, tests, evidence packages, recommendations, reports, APIs, integrations, and beta features are provided "as is" and "as available" except as expressly stated in an Order.

To the maximum extent permitted by law, Provider disclaims all implied warranties and conditions, including merchantability, fitness for a particular purpose, title, non-infringement, quiet enjoyment, accuracy, availability, security, compatibility, and uninterrupted operation.

38. Beta, Preview, Trial, Free, and Evaluation Features

This Section 38 applies to beta, preview, trial, experimental, free, evaluation, proof-of-concept, pre-release, early-access, and no-charge features. It does not apply to the Initial Trial in Section 19A, which is a trial of generally available paid Products and is governed by Section 19A.

Beta, preview, trial, experimental, free, evaluation, proof-of-concept, pre-release, early-access, and no-charge features are not part of Provider's generally available paid Services unless a signed Order expressly says otherwise. They may be changed, limited, suspended, removed, deleted, made paid, or discontinued at any time and may never become generally available.

They are provided without warranty, indemnity, support commitment, service level, data retention commitment, availability commitment, security commitment beyond any non-waivable legal duty, or liability to the maximum extent permitted by law.

Client must not use beta, preview, trial, experimental, free, evaluation, proof-of-concept, pre-release, early-access, or no-charge features for production, regulated, mission-critical, audit-critical, security-critical, privacy-critical, or safety-critical purposes. Client must not process personal information, regulated data, payment data, health data, confidential customer data, or audit-critical evidence through those features unless Provider expressly authorizes that use in writing.

Information about non-public features, betas, previews, roadmaps, experiments, and evaluations is Provider Confidential Information unless Provider publicly releases it.

39. Limitation of Liability

Provider's liability is capped, and the applicable cap depends on what Client bought. Products and subscriptions are sold at a recurring monthly price and carry a monthly cap. Custom Services are sold by project phase and carry a phase cap. The two caps are calculated separately, neither one borrows the other's measure, and neither one is increased by the existence of the other.

39.1 Products, Subscriptions, and the Off Grid Properties

To the maximum extent permitted by law, Provider's total aggregate liability arising out of or related to bug, witness, peachfuzz, any other Product, any subscription, license, hosted service, hosting plan, maintenance plan, support plan, retainer, the Off Grid Properties, or any third-party service used to deliver them will not exceed the fees actually paid by Client to Provider for that Product, subscription, or plan during the one month immediately before the first event giving rise to liability.

That measure is deliberate and matches how these offerings are sold. They are licensed or provided at a recurring monthly price, are used at Client's discretion, are cancellable by Client at the end of a billing period, hold no obligation to Client's customers, and are governed by the warranty disclaimers in Section 37 and the acknowledgements in Sections 8 and 9. One month of fees is the agreed allocation of risk for something priced and cancellable by the month.

Where a Product, licence, or plan is not billed monthly, the measure is the fees actually paid by Client for that Product, licence, or plan during the twelve months immediately before the first event giving rise to liability. Not billed monthly means an annual subscription, a multi-year term, a prepaid period, or a self-hosted licence under Section 21B.5. The measure follows how the thing was sold: a monthly price gives a monthly cap, and an annual or one-time price gives a twelve-month cap.

This is a single aggregate cap. It is not a per-claim, per-incident, per-Order, per-month, or per-year cap, and it does not reset, renew, accumulate, or increase because there is more than one claim, more than one event, more than one Order, more than one Product, more than one billing period, or a continuing or repeated event. All claims by Client and by any person claiming through or on behalf of Client, including Client's affiliates, users, customers, employees, contractors, insurers, and successors, count against the same single cap.

39.2 Custom Services and Deliverables

To the maximum extent permitted by law, Provider's total aggregate liability arising out of or related to custom Services, Deliverables, or a professional services Order will not exceed the

fees actually paid by Client under that Order for the milestone, phase, or portion of the Services giving rise to the claim.

A claim arising from one milestone or phase does not reach fees paid for any other milestone or phase, and payment of a later milestone does not increase the cap available for an earlier one. Where the Order is not divided into milestones or phases, the cap is the fees actually paid by Client under that Order during the twelve months immediately before the first event giving rise to liability.

Within a single milestone or phase this is an aggregate cap, and the sentence above about multiple claims, events, and persons claiming through Client applies to it in the same way.

Nothing in this Section 39.2 makes any fee refundable. Deposits, milestone payments, and the other amounts described in Sections 19, 20, and 45 remain non-refundable on their own terms. This section states the maximum Provider can be ordered to pay in respect of a claim; it does not create a right to a refund, a credit, or a return of fees for work performed, delivered, accepted, or deemed accepted.

39.3 No-Charge and Trial Use

If Client paid no fees under the applicable Order during the applicable measuring period, including during the Initial Trial described in Section 19A, during any free, promotional, credited, discounted, or no-charge period, during use of a beta or preview feature under Section 38, or after the Order ended, Provider's total aggregate liability will not exceed CAD $1,000. The Parties agree this amount is the agreed, adequate, and exclusive monetary remedy for no-charge, trial, beta, and preview use, that it is a real and substantive sum rather than a nominal or illusory one, and that Provider would not offer no-charge, trial, beta, or preview access at all without it.

39.4 The Caps Are Mutual, and What Sits Outside Them

The applicable cap applies to each Party. Provider's total aggregate liability to Client, and Client's total aggregate liability to Provider, are each limited as stated above, and the exclusion of indirect and consequential damages below applies to both Parties equally. Neither Party bears an unlimited exposure to the other except for the matters listed next.

On Provider's side, the cap applies to every claim, cause of action, and obligation of Provider under or related to this Agreement, including Provider's indemnity obligations under Section 42, Provider's warranty obligations under Sections 36 and 37, and any statutory, equitable, or restitutionary claim, to the maximum extent permitted by law.

Nothing in this Section 39 caps, limits, or excludes any of the following, and each of them sits outside every cap stated above:

- Fraud, fraudulent misrepresentation, gross negligence, or wilful misconduct by either Party.
- Client's obligations to pay, including under Sections 19, 20, 21, and 21A, and including the amounts payable on a reversed payment under Section 21A.
- Client's indemnity obligations under Section 41.
- Client's breach of the licence restrictions in Sections 30 and 30B, or of the ownership, payment, and reproduction restrictions in Section 29.
- Either Party's breach of its confidentiality obligations under Section 27.
- Death or personal injury caused by negligence, and any other liability that cannot lawfully be limited or excluded.

The result is a cap that runs both ways and a set of exceptions that run to what each Party actually cares about: Provider cannot be pursued beyond the stated measure for the ordinary risks of supplying software and services, and Client cannot escape paying, indemnifying, respecting the licence, or respecting what it has not paid for.

If a court or arbitrator finds that a cap or exclusion in this Section 39 cannot be applied to a particular claim, that finding applies only to that claim, and every other cap, exclusion, and limitation in this Section 39 continues to apply in full to every other claim.

39.5 Enhanced Cap by Agreement

A Client that requires a higher limit for particular risks may purchase one. Where an Order expressly states an enhanced cap for a defined category of claims, that enhanced cap applies to those claims in place of the cap in Sections 39.1 and 39.2, and the cap in those Sections continues to apply to everything else. A

defined category might be claims arising from breach of confidentiality under Section 27, or from the security obligations in Sections 25 and 25A, stated as a multiple of the applicable cap.

An enhanced cap is priced. It is a transfer of risk from Client to Provider, Provider's fees are set on the allocation of risk in this Agreement as Section 40 states, and an Order that raises the limit without pricing it has not transferred anything.

To the maximum extent permitted by law, Provider will not be liable for indirect, incidental, special, consequential, exemplary, aggravated, punitive, or enhanced damages; lost profits; lost revenue; lost savings; lost business opportunity; lost goodwill; lost data; data restoration costs; business interruption; procurement failure; audit failure; certification failure; regulatory action; customer claim; security incident; or cost of substitute goods or services, even if Provider was advised of the possibility.

The limitations apply regardless of legal theory, including contract, tort, negligence, strict liability, warranty, statute, equity, indemnity, or otherwise.

40. Essential Basis of Bargain

Client agrees that the fees reflect the allocation of risk in this Agreement. Provider would not provide the Services or Products at the stated fees without the warranty disclaimers, liability limits, indemnities, payment obligations, arbitration clause, and scope controls in this Agreement.

41. Client Indemnity

Client will defend, indemnify, and hold harmless Provider and its owners, directors, officers, employees, contractors, agents, affiliates, successors, and assigns from and against all claims, demands, losses, damages, liabilities, penalties, fines, settlements, judgments, costs, and expenses, including reasonable legal fees, arising out of or related to:

- Client Materials.
- Client's products, services, business, customers, users, employees, contractors, vendors, or systems.
- Client's use or misuse of Services, Products, Deliverables, reports, evidence, recommendations, or outputs.

- Client's breach of this Agreement or an Order.
- Client's violation of law, regulation, third-party rights, privacy obligations, security obligations, anti-spam obligations, export controls, platform terms, or industry standards.
- Client's instructions to Provider.
- Client's failure to obtain required consents, permissions, licenses, legal bases, notices, or approvals.
- Client's compliance program, audit, certification, attestation, procurement, or regulator interaction.
- Allegations that Client Materials infringe, misappropriate, defame, violate privacy rights, violate publicity rights, or are unlawful.
- Security incidents, data breaches, credential compromise, or unauthorized access caused by Client systems, Client personnel, Client vendors, Client configurations, Client Materials, or Client instructions.

Provider may participate in the defense with counsel of its choice. Client may not settle a claim in a way that admits fault by Provider, imposes obligations on Provider, restricts Provider's business, or requires payment by Provider without Provider's written consent.

42. Provider IP Indemnity

If a third party claims that a custom Deliverable created by Provider and used as authorized infringes that third party's Canadian or U.S. copyright, Provider will defend Client against that claim and pay final damages awarded or settlements approved by Provider, subject to this Agreement.

Provider has no obligation for claims arising from:

- Client Materials.
- Client instructions.
- Third-party materials.
- Open-source software.
- Products.
- Modified Deliverables.
- Combination with items not provided by Provider.
- Use outside the scope of the Order.

- Continued use after Provider provides a non-infringing alternative or asks Client to stop use.
- Alleged infringement based on business methods, data, content, APIs, compliance frameworks, standards, or general ideas.

Provider may resolve an infringement claim by procuring continued use rights, modifying the Deliverable, replacing the Deliverable, or terminating the affected rights and refunding prepaid unused fees for the affected item. This section states Provider's entire obligation for IP infringement claims.

43. Insurance

Client should maintain insurance appropriate for its business, including cyber liability, technology errors and omissions, commercial general liability, crime/social engineering, data breach, and business interruption coverage.

Provider will maintain insurance only if expressly required by an Order and priced into the engagement.

44. Term and Renewal

This Agreement begins on the effective date of the first Order or acceptance and continues until terminated.

If a subscription begins with an Initial Trial under Section 19A, the term begins on the day the Initial Trial begins, not on the day it converts. The retention window under Section 21B and any rate held under an Order run from that same date. Taking the trial therefore does not shorten a retention window, move a rate lock, or push a renewal date, and the first charge falls at the end of the trial period.

Subscriptions, hosting, maintenance, and support plans renew for successive monthly or annual periods until cancelled.

A monthly plan can be cancelled at any time by Client from its account page on Provider's website, without notice, without a reason, and without contacting Provider. Cancellation takes effect at the end of the period Client has already paid for, and the plan does not renew again. Client keeps full use for the remainder of that period. Nothing is refunded for the remainder of the period, as Section 19 provides.

An annual or multi-year plan renews unless either Party gives written non-renewal notice at least thirty days before the renewal date, unless the Order states a different notice period. During its term, an annual or multi-year plan is not cancellable, as Section 19 provides, because the term is what pays for the capacity, the retention window, and any rate held under the Order.

Renewal fees may change on notice before renewal, except where a rate is held under the following paragraph. Continued use after renewal or fee change constitutes acceptance.

Where an Order or the published plan states a retention or subscription window, the rate Client starts at is held for the length of that window and does not change during it, however Provider's list prices move in the meantime. The rate is held on continuous payment: an account that lapses, is cancelled, or is closed and later resubscribes starts again at the list price current at that time, with a new window and a new held rate running from that date. When a window ends, renewal is priced at Provider's then-current rate for the plan, and that rate is in turn held for the new window. The held rate covers the plan as sold; usage-based fees, overage fees, third-party costs, taxes, and separately ordered work are not covered by it.

Provider holds the rate because custody is only useful if Client can rely on it for the whole window, and a provider able to reprice a dependency at will has not sold custody so much as storage with leverage attached.

45. Termination for Convenience

Either Party may terminate a custom Services Order for convenience on thirty days written notice unless the Order states otherwise.

Upon termination for convenience by Client, Client must pay:

- All fees for work performed.
- All accepted or deemed accepted Deliverables.
- All non-refundable fees.
- All committed, non-cancellable, or approved expenses.
- All third-party costs.
- Any unpaid subscription, hosting, maintenance, or support fees through the end of the then-current term.

- A kill fee equal to 50% of the remaining unpaid project fees, unless the Order states a different kill fee.

The Parties agree that the kill fee is a genuine advance estimate of the capacity, scheduling, remobilization, and lost opportunity costs that early termination causes Provider, and is not a penalty.

Provider is the terminating Party where Provider chooses to stop for its own reasons and Client is not in breach. In that case Client owes only the fees for work Provider performed up to termination, together with committed and non-cancellable third-party costs, and Provider will return any prepaid amount that relates to work Provider has not performed. No kill fee is payable in that case.

That is the only circumstance in which prepaid fees are returned on a termination for convenience, and it applies only where Provider is the terminating Party and Client is not in breach. Where Client terminates, changes its mind, changes direction, cancels, pauses indefinitely, stops responding, runs out of budget, loses its internal sponsor, or takes the work elsewhere, the amounts listed above remain payable in full and nothing is refunded.

Provider may withhold incomplete Deliverables, source code, credentials, transfer assistance, and licenses until all amounts due are paid.

46. Termination for Cause

Either Party may terminate an Order or this Agreement if the other Party materially breaches and does not cure within ten business days after written notice.

Provider may terminate or suspend immediately if:

- Client fails to pay when due.
- Client breaches license restrictions.
- Client creates security, legal, reputational, operational, or platform risk.
- Client uses Services or Products unlawfully or abusively.
- Client asks Provider to violate law, third-party terms, professional obligations, security standards, or ethical constraints.
- Client becomes insolvent, bankrupt, dissolved, or unable to pay debts.

Termination does not relieve Client of payment obligations accrued before termination.

47. Effect of Termination

Upon termination:

- Client must stop using Products and Provider Background IP except for licenses that expressly survive, which include the read-only licence in Section 21B.2B.
- Provider may stop Services, support, hosting, maintenance, access, licenses, and deliverables, other than the read-only licence in Section 21B.2B.
- Client must pay all outstanding amounts immediately.
- Each Party must return or destroy Confidential Information upon request, except archival backups, legal records, audit records, and materials required for dispute resolution or compliance.
- Sections intended to survive will survive, including payment, confidentiality, IP, license restrictions, warranty disclaimers, limitations of liability, indemnities, dispute resolution, governing law, general terms, and the read-only licence in Section 21B.2B, which survives on the terms that Section states.

48. Data Return and Deletion

Upon written request after termination, Provider will use commercially reasonable efforts to export or return Client data in a reasonable format if technically available and if Client has paid all amounts due.

Provider may delete Client data after termination, non-renewal, account closure, nonpayment, or expiry of retention periods. Provider is not required to retain data unless an Order states otherwise.

Client is responsible for maintaining independent backups. Provider is not liable for lost data unless caused by Provider's willful misconduct and subject to the liability cap.

48A. Legal Orders, Abuse Reports, and Infrastructure Requests

Provider may preserve, access, review, suspend, remove, disclose, or retain Client Materials, account information, logs, billing records, abuse reports, security records, or product data when Provider reasonably believes it is required or permitted by law, court order, subpoena, regulator request, payment processor request, telecommunications provider request, cloud provider request, platform policy, abuse investigation, security investigation, or protection of Provider, Client, users, third parties, or infrastructure.

Where legally permitted and commercially reasonable, Provider will attempt to notify Client of compulsory legal process seeking Client information. Provider may delay or omit notice if prohibited by law, if notice could create security risk, if the request relates to abuse or fraud, or if the request is an emergency.

Client will reimburse Provider for reasonable costs, legal fees, vendor fees, employee time, contractor time, and expenses incurred responding to subpoenas, court orders, law-enforcement requests, regulator requests, payment processor requests, telecommunications provider requests, cloud provider requests, third-party claims, or abuse investigations arising from Client's use of Services or Products.

49. Non-Solicitation

During the term and for twelve months after termination, Client will not knowingly solicit for employment or contract work any employee, contractor, or subcontractor of Provider who was involved in the Services, except through general solicitations not targeted at that person.

If Client breaches this section, Client will pay Provider a placement fee equal to 50% of the person's first-year compensation or contractor fees, as a reasonable estimate of recruitment, replacement, and business disruption costs.

50. Independent Contractor

Provider is an independent contractor. Nothing in this Agreement creates an employment, partnership, joint venture, fiduciary, franchise, agency, trustee, or representative relationship.

Provider controls the manner and means of performing Services, subject to the agreed scope. Provider may use employees, contractors, subcontractors, agents, automation, tools, and third-party providers.

51. Force Majeure

Provider is not liable for delay or failure caused by events beyond its reasonable control, including natural disasters, fire, flood, severe weather, pandemic, epidemic, war, terrorism, civil unrest, labor dispute, government action, court order, power failure, internet failure, cloud provider failure, registrar failure, platform outage, supply-chain issue, third-party API failure, cyberattack, denial-of-service attack, malware, ransomware, vulnerability, or other event beyond Provider's reasonable control.

Payment obligations are not excused by force majeure.

52. Export Controls and Sanctions

Client will comply with applicable export control, sanctions, anti-corruption, anti-bribery, and trade compliance laws. Client will not use Services or Products in embargoed jurisdictions, for prohibited end users, for prohibited end uses, or in violation of sanctions or export restrictions.

Client represents that it is not located in, organized under the laws of, or ordinarily resident in a sanctioned jurisdiction and is not on any restricted party list applicable to Provider.

Client will not use Services or Products in violation of anti-bribery, anti-corruption, procurement-integrity, government-contracting, campaign-finance, lobbying, sanctions, or export laws, including laws applicable to U.S., Canadian, provincial, state, municipal, public-sector, and quasi-government customers.

53. Compliance With Laws

Each Party will comply with laws applicable to its own business and performance under this Agreement.

Client is responsible for laws and obligations applicable to Client's business, industry, data, customers, users, products, services, marketing, employment, regulated activities, audit scope,

certification scope, procurement requirements, and use of Deliverables or Products.

Provider is responsible for laws applicable to Provider's business as a technology service provider, subject to Client providing accurate information, lawful instructions, and necessary cooperation.

54. Dispute Resolution

Before arbitration, the Parties will attempt in good faith to resolve disputes through direct executive-level negotiation. A Party must provide written notice describing the dispute and requested resolution. The Parties will meet within ten business days unless they agree otherwise.

If the dispute is not resolved within twenty business days after notice, either Party may start arbitration.

Except for payment collection, injunctive relief, IP misuse, confidentiality breach, security misuse, account suspension, or enforcement of an arbitration award, disputes arising out of or related to this Agreement will be finally resolved by arbitration under the Arbitration Act, 1991 (Ontario), or successor legislation.

The seat of arbitration will be Toronto, Ontario. The arbitration will be conducted in English by one arbitrator. The arbitrator may award damages, costs, legal fees, interest, and equitable relief to the extent permitted by law and this Agreement. The award will be final and binding and may be enforced in any court with jurisdiction.

Either Party may instead bring an individual claim that falls within the monetary jurisdiction of the Ontario Small Claims Court in that court rather than in arbitration. Where a dispute does proceed to arbitration, the Parties intend the process to stay proportionate and accessible: a single arbitrator seated in Toronto may decide a smaller claim on documents and written submissions, and the arbitrator may allocate the arbitrator's fees and the costs of the arbitration between the Parties as the arbitrator considers fair.

For U.S. clients, the Parties intend that any arbitration agreement involving interstate or international commerce also be enforceable under the U.S. Federal Arbitration Act to the extent applicable.

55. Class Action and Jury Trial Waiver

To the maximum extent permitted by law, disputes must be brought only on an individual basis and not as a plaintiff, claimant, class member, or representative in a class, collective, consolidated, mass, private attorney general, or representative proceeding.

To the maximum extent permitted by law, each Party waives the right to a jury trial for disputes arising out of or related to this Agreement.

56. Governing Law and Venue

This Agreement and all Orders are governed by the laws of Ontario and the federal laws of Canada applicable in Ontario, without regard to conflict-of-laws rules.

Subject to the arbitration clause, courts located in Toronto, Ontario will have exclusive jurisdiction for court proceedings arising out of or related to this Agreement. Client consents to personal jurisdiction and venue in those courts. Client waives any objection that Toronto, Ontario is an inconvenient forum.

Client agrees that it will not start, continue, join, or support a court, tribunal, administrative, consumer, class, collective, representative, or other proceeding against Provider in Quebec or any forum outside Toronto, Ontario, except to the extent that a non-waivable law prohibits enforcement of this forum clause. If Client starts a proceeding in another forum, Client must reimburse Provider for reasonable legal fees, travel costs, filing costs, translation costs, administrative costs, and other expenses incurred enforcing this Ontario forum clause, to the maximum extent permitted by law.

No law of Quebec, another Canadian province, a U.S. state, or another country will apply merely because Client is located there, uses the Services or Products there, or serves its own customers there, except to the minimum extent that the law is mandatory and cannot be waived by a business customer.

The United Nations Convention on Contracts for the International Sale of Goods does not apply.

57. Injunctive Relief

Provider may seek immediate injunctive or equitable relief in court for actual or threatened breach involving nonpayment-related suspension, IP misuse, license restrictions, confidentiality, security, credentials, reverse engineering, unlawful use, or harm that may not be adequately remedied by damages.

58. Limitation Period

The Parties agree that this Agreement is a business agreement under the Limitations Act, 2002 (Ontario) and that no Party to it is a consumer. To the maximum extent permitted by law, and except for Provider's claims for unpaid fees, any claim by Client arising out of or related to this Agreement, an Order, the Services, the Products, or the Off Grid Properties must be commenced within one year after the day on which the claim was discovered or ought reasonably to have been discovered. This one-year period applies to every such claim, and the Parties vary and exclude the operation of any other limitation period that would otherwise apply to it, other than the ultimate fifteen-year period in section 15 of the Limitations Act, 2002, which the Parties do not vary.

59. Notices

Notices must be in writing and delivered by personal delivery, courier, registered mail, or email to the addresses stated in the Order or later designated by notice.

Unless an Order states otherwise, notices to Provider must be sent to Deliri Software Inc. at the address stated in Section 1, with a copy by email to the contact address published on the Off Grid Software website. Notices to Client may be sent to the email address associated with Client's account, order, billing contact, or notice contact.

Email notices are effective when sent unless the sender receives an automated bounce-back or delivery failure. Notices for breach, termination, arbitration, or legal claims should also be sent by courier or registered mail when practical.

60. Electronic Signatures and Electronic Records

The Parties consent to electronic signatures, electronic records, electronic notices, online acceptance, click-through acceptance, and electronic contracting where permitted by law.

An electronic signature, typed name, checkbox, online checkout, license activation, invoice payment, continued use, or written approval in an agreed system may evidence acceptance if the surrounding records reasonably identify the accepting Party and accepted terms.

Client is responsible for verifying signer authority, signer identity, internal approval authority, account access, retention of electronic records, and compliance with any law requiring paper records, wet signatures, special consumer disclosures, notarization, witness signatures, or other formalities. Provider does not guarantee that any electronic signature workflow, clickwrap, SMS notice, email notice, or electronic record will satisfy every legal requirement for Client's transaction.

SMS, email, push, webhook, carrier, DNS, registrar, payment, marketplace, and third-party delivery systems are outside Provider's full control. Provider does not guarantee message delivery, timing, carrier acceptance, inbox placement, webhook receipt, marketplace approval, payment settlement, or DNS propagation.

61. Assignment

Client may not assign this Agreement or any Order without Provider's prior written consent.

Provider may assign this Agreement or any Order to an affiliate, successor, purchaser, merger party, acquirer, financing source, or transferee of substantially all relevant assets or business, provided the assignee assumes Provider's obligations.

62. Subcontractors

Provider may use subcontractors, contractors, hosting providers, cloud providers, payment processors, AI tools, development tools, security tools, support tools, and other vendors to perform Services or provide Products.

Provider remains responsible for subcontracted work to the same extent Provider would be responsible if it performed the work directly, subject to this Agreement.

62A. Marketplaces, Resellers, and Third-Party Billing Channels

If Client purchases through a marketplace, reseller, referral partner, procurement portal, app store, cloud marketplace, payment processor, or other third-party billing channel, that third party may impose additional ordering, billing, refund, tax, suspension, renewal, cancellation, marketplace-credit, usage, and procurement terms.

Provider is not responsible for reseller acts or omissions, marketplace approval, marketplace credits, payment processor refunds, marketplace tax calculation, third-party procurement workflows, third-party purchase orders, or third-party billing disputes unless a signed Order expressly states otherwise. If marketplace or reseller terms conflict with this Agreement, this Agreement governs as between Provider and Client, and only a signed Order that expressly names the conflicting term and states that it prevails can change that. Client remains responsible to Provider for the fees, obligations, and restrictions in this Agreement whatever the third-party channel provides, and a term Client accepts from that channel does not bind Provider.

63. No Third-Party Beneficiaries

This Agreement is for the benefit of Provider and Client only. No customer, user, employee, auditor, regulator, vendor, investor, insurer, certification body, or other third party has rights under this Agreement unless expressly stated in a signed writing.

64. Severability

If any provision is invalid or unenforceable, the remaining provisions remain in effect. The invalid or unenforceable provision will be modified to the minimum extent necessary to make it enforceable while preserving the Parties' intent as much as possible.

65. Waiver

A waiver must be in writing and signed by the waiving Party. Failure to enforce a provision is not a waiver. Waiver of one breach is not waiver of another breach.

66. Entire Agreement

This Agreement and applicable Orders are the entire agreement between the Parties regarding their subject matter and replace all prior or contemporaneous discussions, proposals, emails, quotes, presentations, demos, drafts, negotiations, representations, and understandings.

No purchase order, vendor portal term, security questionnaire term, invoice memo, email footer, or procurement document modifies this Agreement unless Provider signs a written amendment expressly accepting that modification.

67. Amendments

Provider may update online Product terms for future renewals, new Orders, new features, or continued Product use after notice. Material changes will not retroactively reduce Client's rights for a prepaid subscription period unless required by law, security, third-party platform changes, or product integrity.

Signed Orders may be amended only by written agreement of the Parties.

68. Interpretation

Headings are for convenience only. "Including" means "including without limitation." "Written" includes electronic writing. "Days" means calendar days unless stated otherwise. Business days exclude Saturdays, Sundays, Ontario statutory holidays, and Canadian federal statutory holidays.

Acceptance

No handwritten signature is required for these Terms to be binding. Client accepts these Terms by accessing, purchasing, subscribing to, downloading, installing, activating, renewing,

paying for, or using the Services or Products, or by accepting an Order, invoice, checkout, quote, or other transaction that references these Terms.

Blink Kernel
Toronto, Ontario, M1C 5H7, Canada
ase.deliri@offgridsoftware.ca