

Noktra Privacy Policy

Effective Date: July 7, 2026

Last Updated: July 7, 2026

Applies to: Noktra and its current and future services

This Privacy Policy explains how Noktra handles personal information when you use our services. It applies across Noktra websites, Cookie, Lockie, Vaultory, dashboards, APIs, Discord integrations, creator tools, paid plans, support channels, beta programs, and future Noktra offerings unless a service-specific privacy notice says otherwise.

Contents

1. Who We Are and Scope
2. Personal Information We Collect
3. How We Use Information
4. Legal Bases and Consent
5. How We Share Information
6. Cookies and Similar Technologies
7. Data Retention
8. Security
9. International Processing
10. Your Privacy Choices and Rights
11. Marketing Communications
12. Children and Young People
13. Third-Party Services
14. Changes to This Policy
15. Contact and Complaints

1. Who We Are and Scope

Noktra ("Noktra," "we," "us," or "our") operates from Ontario, Canada. This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information in connection with Noktra Services, including Cookie, Lockie, Vaultory, Noktra websites, dashboards, applications, APIs, Discord bots, support channels, beta programs, and future services.

Personal information means information about an identifiable person, whether on its own or together with other information. This Policy does not cover third-party services, communities, websites, payment processors, app stores, or platforms that have their own privacy policies. In particular, Discord, GitHub,

and payment processors such as Stripe handle information under their own policies when you use their services.

2. Personal Information We Collect

2.1 Information You Provide

- Account and profile information, such as your name, email address, username, display name, avatar, account identifiers, and settings that you choose to provide or connect.
- Support and communications information, such as emails, help requests, messages, bug reports, feedback, survey responses, attachments, and information you include when you contact us.
- Billing and purchase information, such as the service or plan purchased, purchase date, amount, currency, tax information where required, billing status, invoice references, and payment-processor transaction identifiers. We do not intentionally store full payment-card numbers when payments are handled by a payment processor.
- Creator and project information, such as project names, descriptions, public profiles, project assets, releases, files, licenses, screenshots, version information, download settings, and chosen visibility controls.
- Other information you submit through the Services, including content, comments, configurations, forms, or files.

2.2 Information From Third-Party Accounts and Platforms

When you connect a third-party account or use a platform integration, we may receive information that the platform permits you to share and that is needed to provide the requested connection. For example, Discord may provide platform identifiers, username or display name, avatar, server or community information, permissions, and interaction information. GitHub or another login provider may provide your provider identifier, profile details, and the authorization information needed to support sign-in. The exact information depends on the platform, your settings, and the permissions you approve.

2.3 Information Collected Automatically

- Technical and log information, such as IP address, browser type, device and operating-system information, language, approximate location derived from IP address, request timestamps, pages or features used, referring URLs, error reports, performance information, and security events.
- Cookies, local storage, session identifiers, and similar technologies used to remember preferences, keep you signed in, protect against fraud, measure performance, and understand how services are used.
- Usage and interaction information, such as commands used, bot interactions, feature usage, configuration changes, API request data, rate-limit events, and account activity necessary to operate and secure a Service.
- Security and integrity information, such as account-recovery events, authentication events, abuse reports, anti-fraud signals, file hashes, malware-scan results, and information needed to investigate suspected violations.

2.4 Discord Bot and Community Data

When a Noktra Discord bot is installed or used, we may process Discord user identifiers, server or guild identifiers, channel and role identifiers, bot configuration, command and interaction data, moderation-related data, and other information required for the feature that a server enables. We do not use Discord data to read private content for unrelated purposes. Message content may be processed only when a feature requires it, when a user directly invokes the bot, or when the platform makes it available under applicable platform rules and permissions.

2.5 Files, Downloads, and Creator Content

For creator, upload, and download services such as Vaultory, we may process uploaded files, file names, metadata, descriptions, version information, checksums or hashes, malware-scan results, license details, download activity, project ownership claims, and reports from users. We use this information to host and distribute content, detect harmful files, prevent fraud and abuse, and improve safety.

2.6 AI-Enabled Features

Where a Noktra Service offers AI-enabled features, we may process prompts, files, context, outputs, account information, and technical logs that are necessary to provide, secure, monitor, and improve that feature. Do not submit highly sensitive personal information, confidential business information, or another person's personal information to an AI feature unless the relevant service clearly supports that use. We do not use private user content to train general-purpose AI models unless we clearly tell you and obtain any consent required by law.

3. How We Use Information

We use personal information only for purposes that are appropriate in the circumstances, including to provide, maintain, secure, and improve the Noktra Services. Depending on the Service, we use information to:

- Create, authenticate, administer, and secure Accounts and connected third-party identities.
- Provide requested features, including bot functionality, dashboard access, content hosting, project distribution, downloads, support, and paid benefits.
- Process purchases, manage subscriptions, issue receipts, handle billing questions, prevent fraud, and manage payment disputes.
- Maintain the reliability, security, quality, and performance of the Services; detect bugs; troubleshoot; and protect against abuse, unauthorized access, malware, fraud, and other harmful activity.
- Moderate content and enforce our Terms, service-specific rules, intellectual-property rules, and legal obligations.
- Personalize your experience, remember preferences, and provide relevant service-related information.
- Communicate with you about account activity, security, support, billing, maintenance, product changes, policy updates, and, with the required consent, marketing messages.
- Analyze aggregate or de-identified usage trends to understand how services perform and how to improve them.
- Comply with legal obligations, respond to lawful requests, protect rights and property, and resolve disputes.

4. Legal Bases and Consent

Where privacy law requires a legal basis for processing, we rely on one or more of the following: your consent; performance of a contract with you; our legitimate interests in operating, securing, improving, and protecting the Services; compliance with legal obligations; and protection of rights, safety, or property. Our legitimate interests do not override rights or interests that require stronger protection under applicable law.

Where we rely on consent, you may withdraw it at any time, subject to legal and contractual limits. Withdrawal will not affect processing that occurred before withdrawal, and it may limit features that require the information or permission you withdraw. You may adjust certain permissions in the relevant Service or contact us at contact@noktra.ca.

5. How We Share Information

We do not sell personal information in exchange for money. We may disclose personal information only as described in this Policy, with your direction, with your consent, or as permitted or required by law.

- Service providers that help us operate the Services, such as infrastructure, hosting, content-delivery, database, security, logging, communications, analytics, customer-support, email, and payment-processing providers. They may access personal information only as needed to provide services to us and subject to appropriate contractual or legal safeguards.
- Third-party platforms and integrations when you choose to connect them, use a feature that depends on them, or direct us to share information. For example, information may be exchanged with Discord or GitHub to enable login, bot functionality, or account connections.
- Other users or the public when you choose to make information public, such as a creator profile, project page, release notes, public comments, public content, or publicly visible account details. Public information can be copied or re-shared by others.
- Safety, fraud-prevention, and security partners where needed to detect malicious activity, protect users, investigate abuse, or respond to incidents.
- Professional advisers, insurers, auditors, or transaction partners where reasonably necessary for legal, accounting, compliance, insurance, financing, restructuring, merger, acquisition, or sale of assets.
- Law enforcement, regulators, courts, or other parties when we reasonably believe disclosure is required by law, legal process, enforceable government request, or to protect the rights, safety, security, property, or integrity of Noktra, users, or the public.

6. Cookies and Similar Technologies

We and our service providers may use cookies, local storage, pixels, SDKs, and similar technologies. These tools can be essential for authentication and security, useful for remembering preferences and measuring performance, or optional for analytics or marketing where offered.

You can control cookies through browser or device settings. Blocking some cookies may affect sign-in, security checks, preferences, payment flows, or other parts of the Services. Where we use a consent tool for optional cookies, you can use it to manage the choices offered. We will obtain consent for non-essential cookies where applicable law requires it.

7. Data Retention

We retain personal information for as long as reasonably necessary for the purposes described in this Policy, including to provide the Services, maintain records, meet legal and accounting obligations, prevent fraud, resolve disputes, enforce agreements, and protect security. Retention periods depend on the type of information, the Service, your account status, legal requirements, and the risk associated with deletion or retention.

When information is no longer reasonably needed, we will delete, anonymize, aggregate, or securely isolate it, unless continued retention is required or permitted by law. Deleting an Account or Content does not always remove all copies immediately. For example, information may remain temporarily in backups, logs, fraud-prevention systems, billing records, or legal records before routine deletion or expiration.

8. Security

We use administrative, technical, and organizational safeguards designed to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. Measures may include access controls, encryption in transit where appropriate, logging, monitoring, security testing, least-privilege practices, backups, and vendor review.

No method of transmission or storage is completely secure. You are responsible for protecting your Account credentials, devices, recovery methods, and third-party accounts. If we become aware of a security breach involving personal information, we will investigate and provide notices or reports when required by applicable law.

9. International Processing

Noktra is based in Canada, but our service providers, infrastructure, support tools, and users may be located in other provinces or countries. Personal information may therefore be processed, stored, or accessed outside your province, territory, or country, including in jurisdictions that may have different privacy laws.

When information is transferred internationally, we use reasonable contractual, organizational, and technical safeguards appropriate to the transfer and applicable law. Government authorities in the country where information is processed may have lawful access to it under local law.

10. Your Privacy Choices and Rights

Depending on where you live and applicable law, you may have rights to request access to, correction of, deletion of, portability of, restriction of, or objection to certain processing of your personal information. You may also have rights to withdraw consent, opt out of certain marketing, and complain to a privacy regulator.

To make a request, email contact@noktra.ca with the subject line "Privacy Request." Tell us which Noktra Service is involved, the account email or platform identifier where available, the right you want to exercise, and enough information for us to verify your identity. We may request reasonable verification before responding, and we may limit or decline a request where permitted by law, such as when

responding would reveal another person's information, compromise security, or conflict with a legal obligation.

We aim to respond within the time required by applicable law. If you are dissatisfied with our response, you may have the right to complain to the privacy authority responsible in your location. In Canada, this may include the Office of the Privacy Commissioner of Canada or a relevant provincial privacy authority.

11. Marketing Communications

We may send promotional messages only where permitted by law and, when required, with your consent. Promotional emails will include a way to unsubscribe or manage preferences. You can also contact us at contact@noktra.ca. Please allow a reasonable time for an unsubscribe request to take effect.

You will continue to receive essential service messages, including security alerts, account notices, policy updates, receipts, billing communications, and responses to support requests, even if you opt out of promotional messages.

12. Children and Young People

Noktra Services are not intended for children where use would violate applicable law or the rules of a third-party platform. If you are under the age at which you can consent to personal-information processing where you live, use the Services only with the involvement of a parent or legal guardian where required.

If you believe a child has provided personal information to us without appropriate authorization, contact us at contact@noktra.ca. We will review the request and take appropriate steps consistent with applicable law.

13. Third-Party Services

The Services may link to or integrate with third-party websites, platforms, payment services, marketplaces, applications, social platforms, or content. We are not responsible for the privacy practices, availability, security, or content of those third parties. Review their policies before providing them with personal information or using their services.

14. Changes to This Policy

We may update this Privacy Policy to reflect changes in our Services, data practices, legal requirements, security measures, or user feedback. We will post the updated Policy with a new effective or last-updated date. If a change is material, we may provide additional notice through the relevant Service, email, or another reasonable method. Your continued use after the updated Policy becomes effective is subject to the updated Policy, to the extent permitted by law.

15. Contact and Complaints

Privacy questions and requests

Email: contact@noktra.ca

Website: noktra.ca

Use the subject line "Privacy Request" for access, correction, deletion, consent-withdrawal, or other privacy requests. Include the relevant Noktra Service and account or platform identifier where possible.