

TruNorAI Consultants Ltd.

Master Terms of Use & Privacy Policy

Effective Date: July 2, 2026

SECTION A — TERMS OF USE

Governing Enterprise AI Platforms, Public Web Properties, and Technical Integrations

1. Acceptance of Terms & Discretionary Modifications

These Master Terms of Use ("Terms") govern the access to and utilization of all products, platforms, websites, applications, APIs, software, consulting services, managed services, and technology solutions (collectively, the "Services") provided by TruNorAI Consultants Ltd. ("TruNorAI," "we," "our," or "us").

By accessing, browsing, or integrating any TruNorAI Service or Web Property, you or the entity you represent ("Customer," "you," or "your") explicitly agree to be bound by these Terms. We reserve the right to revise, modify, or update these Terms from time to time at our sole discretion. Your continued use of the Services following the posting of revised Terms means that you accept and agree to the changes. You are expected to check this framework periodically to stay apprised of binding changes.

2. Scope of Services & Website Availability

These Terms apply broadly to all standard enterprise software, custom white-label deployments, strategic AI consulting, and public website resources deployed by TruNorAI. This includes, but is not limited to, the following domains:

2.1 Software & AI Platforms

- Web-based enterprise applications and workflow automation systems.
- AI-powered document intelligence and knowledge management platforms.
- Procurement, RFQ automation, and supplier management tools.
- ERP-integrated analytics systems and business intelligence dashboards.
- M&A and due diligence artificial intelligence suites.

2.2 APIs & Integrations

- REST APIs and AI inference services.
- Secure data connectors and ERP/CRM integrations.
- Identity provider integrations (SSO/OIDC) and OEM/embedded AI services.

2.3 Custom & Enterprise Solutions

- Custom-developed software architecture and white-label deployments.
- On-premise installations, private cloud deployments, and managed hosting services.
- Strategic AI consulting and targeted implementation services.

Our public-facing digital platforms are generally provided free of charge; however, TruNorAI does not guarantee that our web interfaces or public content will always be available or uninterrupted. We may suspend, withdraw, or restrict the availability of all or any part of our digital portals for technical, business, or operational reasons.

3. Age Restrictions & Acceptable Use Policy

The Services and public web assets provided by TruNorAI are strictly intended for and applicable only to individuals who are eighteen (18) years of age or older (or the legal age of majority in your jurisdiction). If you are under the age of 18, you are expressly prohibited from utilizing our platforms, establishing user accounts, or transmitting inquiries.

Customers and users are strictly prohibited from utilizing the Services for unlawful purposes. Prohibited actions include, but are not limited to: deploying malware, malicious code, or harmful content; attempting unauthorized penetration testing, vulnerability scanning, or system access; reverse-engineering proprietary AI inference models, algorithms, logic mechanisms, or neural weights; circumventing established security and authentication mechanisms; or using any part of the content on our properties for commercial resale without obtaining an explicit commercial license from TruNorAI.

4. Enterprise Data & Confidential Information

In the course of providing the Services, TruNorAI may process sensitive and proprietary enterprise information. All such information submitted by the Customer to the Services is defined as "Customer Data," encompassing customer documents, procurement data, bills of materials (BOMs), ERP exports, financial records, M&A documentation, corporate strategy materials, and trade secrets.

4.1 Ownership of Customer Data

The Customer explicitly retains full, unencumbered ownership of all right, title, and interest in and to all Customer Data. TruNorAI claims no intellectual property rights or ownership stakes over Customer Data.

4.2 Confidentiality Obligations

TruNorAI agrees to strictly maintain the confidentiality of Customer Data. We shall utilize Customer Data solely for the purpose of delivering the contracted Services. Disclosure is strictly prohibited, except to authorized subprocessors operating under equivalent confidentiality obligations, or as legally mandated by a competent authority. These confidentiality obligations shall survive the termination or expiration of any agreement.

5. Data Processing Roles

Unless expressly superseded by a customized written agreement, the Customer acts as the Data Controller (or "Business" under applicable U.S. privacy frameworks), and TruNorAI acts as the Data Processor (or "Service Provider"). Processing activities are governed by these Terms, any applicable Data Processing Agreement (DPA), and Master Service Agreements executed between the parties.

6. Intellectual Property Ownership & Digital Content Usage Rules

TruNorAI (or its explicit licensors) expressly retains exclusive ownership of all Services, including foundational software, AI models, algorithms, interface layouts, documentation, codebases, trademarks, and branding assets. These materials are protected by international copyright, trademark, and trade secret laws. Any custom intellectual property developed specifically for a Customer will be governed by the precise terms defined in a separate Statement of Work (SOW) or Enterprise Agreement.

Users may print one copy or download extracts of public documentation or web pages solely for personal use or internal organizational evaluation. However, you must not modify paper or digital copies in any way, separate illustrations or graphics from accompanying text, or remove corporate branding. If any digital asset is used in breach of these provisions, your right to use our Services ceases immediately, and you must return or destroy any unauthorized copies.

7. Reliance on Posted Information

The content published on TruNorAI's public-facing platforms and marketing portals is provided solely for general business information purposes. It does not amount to definitive technical, legal, financial, or operational advice upon which you should rely. You must obtain specialist or professional advice prior to taking, or refraining from, any material corporate action based on public site content. While we make reasonable, continuous efforts to update information, we provide no express or implied guarantees that the web content is completely accurate, flawless, or up to date.

8. AI Processing & Model Usage

8.1 Enterprise Data Segregation

To ensure robust security and data integrity, all Customer Data is logically segregated by tenant architecture. Data is strictly siloed, never shared between distinct customers, and never utilized for the training of generalized, public-facing AI models without explicit, prior written authorization from the Customer.

8.2 AI Output Disclaimer

Artificial Intelligence generated outputs are intended to serve as advanced decision-support mechanisms. Due to the probabilistic nature of AI, outputs may occasionally contain anomalies or inaccuracies. Customers are responsible for instituting human-in-the-loop validation processes prior to making material business decisions based on AI outputs.

9. Security & Safeguards

TruNorAI implements comprehensive, enterprise-grade security protocols aligned with leading industry frameworks to protect against unauthorized access, alteration, or destruction of data.

- **Technical Controls:** Enforcement of TLS 1.2+ encryption in transit and AES-256 (or equivalent) encryption at rest. Implementation of granular role-based access controls (RBAC), secure identity provider frameworks (SSO/OIDC/SAML), comprehensive audit logging, tenant isolation, and stringent cryptographic key management.
- **Organizational Controls:** Mandatory confidentiality agreements for all personnel, rigorous security awareness training, periodic access reviews, structured third-party vendor risk management frameworks, and a formalized incident response framework.
- **Infrastructure Controls:** Deployment within highly secure cloud environments featuring advanced network segmentation, continuous vulnerability monitoring, persistent firewall isolation, and disciplined patch management routines.

10. Limitation of Liability

To the maximum scope permitted under prevailing jurisprudence, the Services are provided "as is" and "as available." TruNorAI disclaims all statutory or implied warranties, including merchantability or fitness for a particular purpose. In no event shall TruNorAI's cumulative, aggregated liability for any legal claims arising from or relating to the use of our services or platforms exceed the total subscription fees paid by the Customer within the twelve (12) month period immediately preceding the event that catalyzed the claim.

11. Governing Law

These Terms, and all subsequent legal contentions or disputes arising out of or related to them, shall be governed by the legal frameworks specified in your active enterprise agreement. In the absence of an executed specialized master agreement, the laws of the Province of British Columbia, Canada, shall govern exclusively.

SECTION B — PRIVACY POLICY

Global Data Protection, Tracking Disclosures, and Recruitment Privacy Framework

1. Regulatory Overview

This Privacy Policy outlines the global privacy standards applicable to all TruNorAI Services. We are committed to processing personal and enterprise data in alignment with major global privacy frameworks, including but not limited to the General Data Protection Regulation (GDPR), UK GDPR / Data Protection Act 2018, the California Consumer Privacy Act (CCPA/CPRA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Singapore's PDPA, Hong Kong's PDPO, and Japan's APPI.

2. Scope of Applicability & Collected Information Categories

This Privacy Policy applies uniformly to (a) website visitors exploring our public digital properties, (b) active or prospective enterprise customers, business partners, or service providers, and (c) job applicants seeking career opportunities with TruNorAI. We process data within the following operational categories:

- **Public Communications & Requests:** Names, corporate email profiles, corporate telephone numbers, and specific message text voluntarily provided via our contact portals, query submissions, or customer support channels.
- **Technical Telemetry & Device Data:** When navigating our properties, we automatically log information via background tracking arrays. This encompasses your Internet Service Provider (ISP), referring and exit URLs, localized device types, browser configurations, software version profiles, system logs, unique user identifiers, IP addresses, country codes, language settings, and active time zones.
- **Mobile & Deployed Application Metrics:** For deployed enterprise mobile arrays or embedded modules, we track authorized device IDs, crash analytics, push notification tokens, and permission-based hardware access (e.g., local storage or camera access) explicitly granted by the user.
- **Job Applicant Portfolios:** If applying for employment within TruNorAI, we collect comprehensive candidate files, including personal contact vectors, images/photographs, government identifications (social security equivalents or driver licenses), citizenship/visa standing, background checks, educational histories, academic grades, professional certifications, past work backgrounds, security clearances, and relocation allowances.

3. Detailed Cookie Framework and Web Beacons

To optimize site operations, ensure infrastructure security, and tailor our professional digital experiences, TruNorAI deploys cookies and similar digital identifiers. You can toggle or refuse cookies inside your browser parameters, though certain elements of our digital portals may become restricted. We categorize our cookie matrices as follows:

- **Essential Cookies:** Critical markers necessary to maintain basic site stability, secure sign-in verification, session validation, and core performance mechanics. These cannot

be deactivated within our user control interfaces.

- **Browser & Functional Cookies:** These improve user interactions by remembering your stylistic preferences, language choices, and previously input authentication profiles so parameters do not need to be repeatedly re-entered.
- **Web Beacons / Pixel Tags:** Small transparent graphic strings deployed inside specific landing elements to compile aggregate statistical telemetry regarding web traffic, loading latency, error configurations, and overall visitor patterns.
- **Targeting & Analytical Cookies:** Records your specific journey milestones and link interactions, enabling TruNorAI to structure updates, features, and marketing insights matching corporate interests.

4. Third-Party Web Analytics (Google Analytics)

Our public properties utilize Google Analytics, a professional suite provided by Google LLC, to gather aggregate behavioral intelligence. Google Analytics relies on first-party cookies to record visitor frequency, origin regions, and journey paths. As part of this process, your IP address is logged to deduce generalized regional blocks (such as country, state, or city location blocks) to contextualize web engagement.

To review Google's underlying privacy rules, visit their official corporate disclosures. If you desire to completely opt out of tracking via Google Analytics across all web entities, you may download and install the official "Google Analytics Opt-out Browser Add-on" provided by Google.

5. Purpose of Processing and Lawful Bases

We process data under recognized legal pillars: the performance of an active contract, the execution of legal statutory obligations (such as right-to-work visa validations, tax filings, or whistleblower management), the pursuit of legitimate commercial interests (ensuring system security, preventing fraudulent activity, and testing system updates), or based upon your unambiguous, explicit consent.

6. Information Sharing, Data Siloing, and Commercial Restriction

TruNorAI does not sell, lease, or distribute personal or corporate data to data brokers or commercial marketing arrays. Data is only shared under protective, contractually bound parameters with: (1) TruNorAI affiliated entities and internal business units, (2) contractually verified third-party data processors operating cloud hosting infrastructure or authentication systems, (3) legal advisors, external audit teams, or prospective corporate buyers in the event of an asset or business sale, or (4) regulatory, law enforcement, or judicial entities where explicitly mandated by global statutory requirements.

7. International Transfers and Foreign Government Access

TruNorAI utilizes distributed enterprise nodes and secure cloud hubs (including primary nodes within Canada, the United States, or the European Economic Area). When personal profiles originate from regulated areas (e.g., the EEA or UK) and cross international borders, we utilize recognized transfer frameworks, including Standard Contractual Clauses (SCCs).

Be advised that data stored internationally may be subject to localized foreign laws and could be accessible by foreign courts, regulatory entities, and national security frameworks under legal domestic mandates.

8. Retention Lifecycles and Data Subject Rights

Information is preserved only for the duration required to satisfy active contractual profiles, active professional recruitment windows, or mandatory statutory records periods. Afterward, data undergoes deep cryptographic purging, secure erasure, or permanent anonymization.

Depending on your operational jurisdiction, you may hold distinct legal rights regarding your personal profiles. These include the right to access your records, correct inaccuracies, request absolute deletion, port records, restrict processing paths, or limit the use of sensitive classifications. To trigger a formal request, contact our Privacy Office.

9. Breach Resolution Protocol

In the event of a confirmed security compromise impacting your stored profiles, TruNorAI executes immediate containment protocols. We commit to conducting deep forensic investigations, notifying impacted customers and users without undue delay, and updating required international privacy authorities within the strict timelines mandated by applicable local laws.

10. Privacy Officer Contact Information

For inquiries, compliance documentation requests, or to exercise data rights, please contact our dedicated Privacy Office:

TruNorAI Consultants Ltd.
British Columbia, Canada
Corporate Web: <https://trunorai.com>
Inquiries & Intake: privacy@trunorai.com