TETRIX LABS LIMITED

JOROMI AI

COOKIE POLICY

This Cookie Policy explains how Tetrixx Labs uses cookies and related tracking technologies in connection with JOROMI AI, its Enterprise AI Operating System, and how users and enterprise customers can manage their preferences.

Enterprise Cookie Policy

Prepared for Enterprise Customers, Regulators, and Compliance Review

Effective Date: 14th July 2026

1. Introduction

This Cookie Policy explains how Tetrixx Labs ("Tetrixx Labs," "we," "us," or "our") uses cookies and related tracking technologies across JOROMI AI, our Enterprise AI Operating System, and the websites, portals, and applications through which it is accessed and administered.

Transparency about how tracking technologies operate is treated as a baseline expectation for an enterprise platform, not a courtesy. Enterprise customers evaluating JOROMI AI for deployment across regulated environments — government, financial services, healthcare, and similarly sensitive sectors — need a clear account of what is tracked, why, and under what controls, in language that supports their own procurement and compliance review rather than obscuring it. This Policy is drafted with that audience in mind.

Our approach to cookies reflects the same principles that govern the rest of the Platform: Privacy by Design, meaning tracking technologies are scoped to a defined purpose rather than deployed by default; Security by Design, meaning cookies used for authentication and session integrity are subject to the same technical safeguards as the rest of the Platform's identity infrastructure; and a commitment to giving users meaningful, granular control over non-essential tracking wherever applicable law requires or good practice recommends it.

Relationship to Our Privacy Policy

This Cookie Policy should be read together with the JOROMI AI Privacy Policy, which governs the broader collection and processing of personal data across the Platform. Where this Policy addresses the specific mechanics of cookies and tracking technologies, the Privacy Policy addresses the fuller scope of data categories, legal bases, retention, international transfers, and user rights. In the event of any conflict between the two documents on a matter specific to cookies, this Policy governs.

2. Scope

This Policy applies to cookies and similar tracking technologies deployed across the full range of digital properties through which JOROMI AI is delivered and supported, including:

- Our public marketing and corporate websites
- Customer portals used to manage accounts, billing, and support requests
- The JOROMI AI enterprise cloud platform, including all constituent modules
- Mobile applications, where made available
- APIs, to the limited extent that API access involves browser-based authentication flows
- The Developer Platform and associated developer portals
- Administrative dashboards used by enterprise customer administrators
- Product documentation websites
- Event registration portals for webinars, conferences, and similar activities

Where an enterprise customer accesses the Platform through a private, dedicated, or hybrid deployment, certain cookies described in this Policy — particularly analytics and marketing-related technologies — may not apply, as further explained in Section 8 (Enterprise Deployments).

3. Definitions

Term	Definition
Cookies	Small text files placed on a user's device by a website or application, used to store information for later retrieval by that site or a third party.
First-Party Cookies	Cookies set directly by the website or platform the user is visiting, in this case Tetrixx Labs' own domains.
Third-Party Cookies	Cookies set by a domain other than the one the user is visiting, typically placed by a service provider engaged by Tetrixx Labs, such as an analytics or identity provider.
Session Cookies	Temporary cookies that are deleted automatically when the browser session ends.
Persistent Cookies	Cookies that remain on a device for a defined period, or until manually deleted, in order to retain information across multiple visits or sessions.
Web Beacons	Small, often invisible graphic images embedded in a webpage or email, used to confirm that content has been viewed or opened.
Pixel Tags	A form of web beacon used to track user interaction with a webpage or communication, sometimes referred to as a tracking pixel.
SDKs	Software Development Kits: code libraries embedded within mobile or desktop applications that can collect usage and diagnostic data in a manner functionally similar to cookies.
Local Storage	Browser-based storage, such as HTML5 Local Storage, that retains data on a user's device without the size and expiry constraints of a traditional cookie.
Browser Storage	A collective term encompassing Local Storage, IndexedDB, and other client-side storage mechanisms made available by modern browsers.
Tracking Technologies	A collective term used in this Policy to refer to cookies, web beacons, pixel tags, SDKs, local storage, and any comparable technology that collects or stores information on or from a user's device.
Analytics Technologies	Tracking technologies specifically deployed to measure usage, performance, and engagement, as distinct from those used for authentication or security.
Device Identifier	A unique or semi-unique value associated with a particular device, used to recognize that device across sessions or visits.

4. Technologies We Use

We use a defined set of tracking technologies, each selected for a specific technical or operational purpose rather than deployed indiscriminately. The table below sets out the technologies in use and the function each performs within the Platform.

Technology	Function
HTTP Cookies	The standard cookie mechanism used for authentication, session state, and basic preference storage across our websites and the Platform.
Session Cookies	Maintain a user's authenticated state and workspace context for the duration of a single browser session.
Persistent Cookies	Retain settings such as language, consent choices, and login persistence across multiple visits, subject to the retention periods set out in our cookie inventory.
HTML5 Local Storage	Stores larger volumes of interface state — such as dashboard layout or in-progress workflow configuration — directly in the browser, reducing the need for repeated server requests.
IndexedDB	Supports more complex client-side data storage requirements within certain Platform modules, such as caching search indices or draft content for offline resilience.
Web Beacons and Pixel Tags	Used sparingly, primarily in marketing emails and on public-facing websites, to confirm delivery and engagement rather than within the enterprise platform itself.
JavaScript Tags	Load analytics, security, and functional scripts required for the website or Platform to operate as intended.
SDKs	Embedded within mobile applications, where available, to support authentication, diagnostics, and usage analytics equivalent to their web-based counterparts.
Device Fingerprinting	Used in a limited capacity, where enabled, as an additional security signal for fraud and abuse detection, rather than for behavioural tracking or advertising.
Authentication Tokens	Cryptographically signed tokens issued upon login, used to verify a user's identity on subsequent requests without repeated credential submission.
Security Tokens	Short-lived tokens used to protect specific actions — such as form submissions or administrative changes — against cross-site request forgery and similar attacks.

5. Categories of Cookies

We classify cookies and related tracking technologies into six functional categories. The categories that apply to a given user depend on whether they are interacting with our marketing websites or the enterprise platform itself, as noted throughout this section.

5.1 Strictly Necessary Cookies

These cookies are essential to the operation of the Platform and our websites, and cannot be disabled without materially affecting functionality. Because they are necessary to provide a service that users have specifically requested, they do not require consent under applicable law, as described further in Section 9 (Cookie Consent).

- Authentication and secure login, including credential verification and session establishment
- Session management, maintaining a user's authenticated state as they navigate the Platform
- Load balancing, directing traffic across our infrastructure to maintain availability
- Enterprise identity and Single Sign-On (SSO), supporting federated login through a customer's identity provider
- Fraud prevention and security controls, detecting and blocking unauthorized access attempts
- Infrastructure resilience, supporting failover and continuity of service during technical incidents

5.2 Functional Cookies

Functional cookies remember choices a user has made in order to deliver a more consistent and personalized experience across sessions. These are not strictly required for the Platform to operate, but disabling them will cause preferences to reset on each visit.

- Language and regional preferences
- Interface theme, such as light or dark mode
- Dashboard layout and saved views within Business Intelligence and Analytics modules
- Accessibility settings, such as font size or contrast adjustments
- User interface customization applied by an individual user or an enterprise administrator
- Workspace settings, including default Tenant or project selection
- Other saved preferences configured by the user within their account settings

5.3 Analytics Cookies

Analytics cookies help us understand how the Platform and our websites are used, in order to identify friction points, prioritize product investment, and measure the effectiveness of new features. We use analytics data in aggregate form for these purposes and do not use it to build individual advertising profiles.

- Platform usage volume and patterns across modules
- Feature adoption following a release
- Navigation patterns and click paths through the interface
- Session duration and frequency of return visits
- Error frequency, to identify and prioritize defects
- Broader performance and engagement trends over time

5.4 Performance Cookies

Performance cookies are closely related to analytics cookies but are focused specifically on the technical health of the Platform rather than user behaviour. They help us identify and resolve issues affecting speed, availability, and reliability.

- Measuring page and application response times
- Monitoring service availability and uptime
- Assessing infrastructure and resource utilization under varying load
- Supporting reliability monitoring and early detection of degraded performance

5.5 Security Cookies

Security cookies operate alongside our strictly necessary cookies but serve a more targeted purpose: identifying and mitigating threats to the Platform and its users. These cookies are considered essential and are treated accordingly for consent purposes.

- Threat detection and anomaly identification across login and session activity
- Session validation, confirming that a session has not been hijacked or tampered with
- Account protection, including step-up authentication triggers
- Bot detection and abuse prevention on public-facing forms and login pages
- Risk analysis supporting adaptive authentication decisions
- Preservation of authentication integrity across distributed infrastructure

5.6 Advertising and Marketing Cookies

Advertising and marketing cookies, where used, are deployed exclusively on our public marketing websites — for example, to measure the performance of a campaign that brought a visitor to our site — and are never deployed within an enterprise customer's authenticated Workspace or Tenant.

> **No Behavioural Advertising Within the Platform**
>
> Enterprise customer Workspaces are not used for behavioural advertising, and no data generated through a customer's use of JOROMI AI is shared with advertising networks. Any advertising or marketing cookies described in this Policy relate solely to visits to our public, unauthenticated marketing websites.

6. Why We Use Cookies

Taken together, the technologies described above support the following purposes:

1. Enabling secure authentication and maintaining session integrity across the Platform
2. Supporting core AI platform functionality, including maintaining context within AI Agent Studio and workflow sessions
3. Facilitating enterprise identity management, including SSO and federated login
4. Delivering a personalized user experience consistent with a user's saved preferences
5. Measuring platform usage and feature adoption through analytics
6. Informing product improvement and prioritization decisions
7. Supporting reliable delivery of AI inference and related services at enterprise scale

8. Monitoring for security threats and responding to suspicious activity
9. Preventing fraud and abuse across authentication and account management flows
10. Supporting compliance with applicable legal and regulatory obligations
11. Improving the operational efficiency of our infrastructure and support functions

7. Third-Party Technologies

Certain tracking technologies on our websites and within the Platform are provided by third parties that support specific functions we do not operate ourselves. These include:

- **Identity Providers:** Support Single Sign-On and federated authentication where an enterprise customer connects its own identity provider to the Platform.
- **Cloud Infrastructure Providers:** Underlie the hosting, content delivery, and load balancing that make certain performance and security cookies necessary.
- **Analytics Services:** Provide the aggregated usage measurement described in Section 5.3, typically through a combination of first- and third-party cookies.
- **Payment Processors:** Deploy cookies or equivalent technologies necessary to process billing transactions securely.
- **Enterprise Integrations:** Third-party systems that an enterprise customer connects to their Tenant, which may set their own cookies when accessed through an embedded interface.
- **Customer-Authorized Applications:** Marketplace applications or connectors that a customer elects to enable within their Workspace, subject to that provider's own tracking practices.

Technologies deployed by third parties remain subject to that third party's own privacy and cookie policies, which we encourage users to review. We select third-party providers with reference to their own security and privacy commitments, but we do not control, and are not responsible for, the specific tracking practices of independently operated third-party services.

8. Enterprise Deployments

Enterprise customers retain a meaningful degree of control over how cookies and related technologies operate within their own Tenant, consistent with the broader administrative capabilities described in the JOROMI AI Privacy Policy. Depending on their deployment model, enterprise administrators may:

- Configure authentication methods, including SSO, multi-factor authentication, and session timeout policies
- Manage which functional and analytics cookies are enabled within their Tenant, where configurable at the Workspace level
- Configure their own identity provider for federated login, replacing certain first-party authentication cookies with tokens issued by that provider
- Deploy the Platform within a private or hybrid cloud environment, in which case marketing and certain thirdparty analytics technologies described in this Policy do not apply
- Establish authentication policies governing session duration, device trust, and re-authentication triggers
- Apply browser and network-level restrictions consistent with their own organizational security policies

Where an enterprise customer disables or restricts a functional or analytics cookie, certain convenience features — such as saved dashboard layouts or personalized recommendations — may not operate as intended. Strictly necessary and security cookies described in Sections 5.1 and 5.5 cannot be disabled without affecting the customer's ability to authenticate and use the Platform securely.

9. Cookie Consent

Where applicable law requires consent before non-essential cookies are set, we obtain that consent through a cookie banner presented on first visit to our websites, together with a preference centre that allows granular selection by category.

- **Consent Banners:** Presented to visitors on our public websites before any non-essential cookie is set, describing the categories of cookies in use and linking to this Policy.
- **Preference Centres:** Allow a visitor to accept or reject cookies by category — functional, analytics, and advertising — rather than on an all-or-nothing basis.
- **Consent Withdrawal:** A user may withdraw previously given consent at any time through the preference centre, after which the relevant non-essential cookies will no longer be set on future visits.
- **Regional Legal Requirements:** Consent mechanisms are calibrated to the requirements applicable in the visitor's jurisdiction, including the EU and UK ePrivacy rules underpinning the GDPR and UK GDPR cookie requirements, and the opt-out and “do not sell or share” mechanisms applicable under the CCPA/CPRA.

Strictly Necessary Cookies

Strictly necessary and security cookies described in Sections 5.1 and 5.5 do not require consent under the ePrivacy rules, the GDPR, or equivalent frameworks, because they are necessary to provide a service the user has specifically requested. These cookies are not included in the preference centre's opt-out controls.

Within the authenticated enterprise platform, consent to functional and analytics cookies is generally addressed at the organizational level through the enterprise customer's agreement with Tetrixx Labs and the administrative controls described in Section 8, rather than through a per-user consent banner, consistent with standard enterprise software practice.

10. Managing Cookies

In addition to the preference centre described in Section 9, users can manage cookies through the following methods:

- **Browser Controls:** Most browsers allow users to view, delete, and block cookies, either universally or on a persite basis, through their settings menu.
- **Rejecting Optional Cookies:** Non-essential cookies may be rejected at the point of the initial consent banner or subsequently adjusted through the preference centre.
- **Deleting Existing Cookies:** Users may delete cookies already stored on their device through their browser settings; this will typically require re-authentication on the next visit.
- **Disabling Third-Party Cookies:** Most modern browsers offer a setting to block third-party cookies specifically, while continuing to allow first-party cookies necessary for core functionality.
- **Mobile Application Settings:** Where SDK-based tracking is used within a mobile application, equivalent controls are typically available through the device's operating system privacy settings.
- **Withdrawing Consent:** As described in Section 9, consent may be withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal.

Disabling or deleting cookies may affect the availability or performance of certain features. Disabling strictly necessary or security cookies in particular is likely to prevent successful authentication and should generally be avoided by users who wish to continue using the Platform.

11. Data Protection and Security

Information collected through cookies and related tracking technologies is protected using the same enterprise-grade security controls that apply to the rest of the Platform, including:

- **Encryption:** Cookie values and associated tokens are transmitted over encrypted connections and, where persisted server-side, encrypted at rest.
- **Access Controls:** Access to cookie-derived data, such as session and analytics records, is restricted on a rolebased, need-to-know basis.
- **Identity Management:** Authentication cookies and tokens are issued and validated through our centralized Identity & Access Management infrastructure.
- **Secure Transmission:** Cookies marked as secure and HTTP-only are used where appropriate to reduce exposure to interception or client-side scripting attacks.
- **Security Monitoring:** Authentication and session activity associated with cookies is monitored for anomalous patterns consistent with our broader security program.
- **Logging and Audit:** Relevant cookie-related events, such as session creation and termination, are logged in a manner consistent with our audit and governance controls.
- **Governance Controls:** Use of analytics and functional cookies is subject to internal review consistent with the Privacy by Design principles described in Section 1.

12. International Data Transfers

Information collected through cookies, including device and usage identifiers, may be processed by Tetrixx Labs and our third-party service providers in countries other than the one in which a user is located. Where this involves a transfer of personal data across borders, we apply safeguards consistent with those described in our Privacy Policy, including:

- Standard Contractual Clauses (SCCs) for transfers originating in the European Economic Area
- The UK International Data Transfer Addendum, applied alongside the SCCs for transfers originating in the United Kingdom
- Data Processing Agreements with third-party providers whose technologies are described in Section 7
- Encryption of data in transit between regions
- Regional hosting options for enterprise customers with specific data residency requirements
- Other cross-border transfer mechanisms recognized under applicable law, including reliance on adequacy decisions where available

13. Compliance

This Cookie Policy is designed to support alignment with the following privacy and ePrivacy frameworks. Except where an independent certification is expressly stated elsewhere by Tetrixx Labs, references below describe the design objectives of our consent and tracking practices, and should not be read as a claim of formal certification or regulatory approval.

Framework	Relevance to This Policy
EU GDPR and ePrivacy Rules	Consent mechanisms for non-essential cookies are designed with reference to the consent standard required under the ePrivacy Directive as implemented alongside the GDPR.
UK GDPR and PECR	Equivalent consent and transparency practices are applied to visitors and users located in the United Kingdom.
Nigeria Data Protection Act (NDPA)	Cookie-related processing is designed to align with the NDPA's requirements applicable to online tracking and consent.
CCPA / CPRA (California)	Preference centre controls support applicable opt-out rights, including “do not sell or share” mechanisms where triggered by our use of analytics or advertising cookies.
Brazil LGPD	Cookie consent and disclosure practices are designed with reference to LGPD principles applicable to online tracking.
PIPEDA (Canada)	Consent and disclosure practices are designed to align with Canadian federal privacy principles where applicable.
POPIA (South Africa)	Cookie-related processing is designed to align with South African data protection principles where applicable.

14. Changes to This Policy

We review this Cookie Policy periodically and may update it to reflect changes in the tracking technologies we use, our third-party service providers, or applicable law. The “Effective Date” at the top of this Policy indicates when it was last revised.

Where a change is material — for example, the introduction of a new category of tracking technology or a change to the third-party providers described in Section 7 — we will provide notice through one or more of the following channels, as appropriate: an updated notice on our website, an in-Platform notification, or direct communication to enterprise customer administrators. Where required by applicable law, we will refresh consent before applying a material change to non-essential cookies. Continued use of our websites or the Platform following the effective date of an updated Policy constitutes acceptance of the changes, to the extent permitted by applicable law.

15. Contact Information

Questions or requests regarding this Cookie Policy may be directed to:

Function	Contact
Privacy Office	[Insert Privacy Office Email Address]

Data Protection Officer	[Insert DPO Name and Email Address, if applicable]
Legal Department	[Insert Legal Department Email Address]
Security Team	[Insert Security Team Email Address / security.txt link]
General Enquiries	[Insert General Contact Email Address]
Website	[Insert Website URL]
Registered Office	[Insert Registered Office Address]

Effective Date: [Insert Effective Date] | Version: [Insert Version Number]

JOROMI AI — The AI Operating System for Modern Enterprises.