SNOVASYS
We Love To Help You Succeed

Communication Terms

SECTION 1 — INTRODUCTION, PURPOSE & SCOPE

1.1 Purpose of this Document

This document establishes the comprehensive, integrated, and binding **Terms, Notices, Disclaimers, and Policies** governing all forms of communication, interaction, data exchange, monitoring, logging, security processing, and electronic activity involving, originating from, or directed to **Snovasys Software Solutions Ltd** and its associated entities ("the Company").

These Terms are intended to:

- define acceptable and prohibited behaviours;
- clarify the operational and legal nature of communications;
- formalise monitoring, security, and audit practices;
- delineate liabilities, obligations, rights, and limitations;
- support compliance with applicable laws in the United Kingdom, India, and other relevant jurisdictions;
- protect the Company's interests, assets, systems, infrastructure, and personnel;
- ensure transparency and consistency across all communication methods.

These Terms apply broadly and shall be interpreted expansively to ensure full protective coverage in all relevant contexts.

1.2 Nature of the Document

This document functions as a **multi-dimensional legal and governance framework**, integrating aspects of:

- communications policy,
- cybersecurity policy,
- acceptable use policy,
- privacy and data processing notices,
- monitoring and surveillance disclosures,
- IT governance guidelines,
- professional conduct guidelines,
- system-use terms and conditions,
- operational disclaimers.

It operates as a **multi-layered protective instrument** governing:

- internal communications,
- external communications,
- verbal, written, electronic, or automated exchanges,
- business, operational, and technical interactions,
- incidental or informal messages,
- planned and unplanned communications.

These Terms are designed to protect both the Company and Users by providing clarity and predictability regarding the handling of communications and data.

1.3 Channels Covered

Unless expressly excluded, these Terms apply to **all communication and interaction channels**, whether now existing or introduced in the future, including without limitation:

Digital & Written Channels

- Email
- In-app messaging
- Ticketing and helpdesk systems
- CRM-based communication
- ERP and HRMS platforms
- Portals, dashboards, and SaaS products
- Electronic forms, uploads, submissions, and file transfers

Real-Time & Voice/Video Channels

- Voice calls (mobile, VoIP, landline)
- Video calls and conferencing
- Online meetings and webinars
- Screensharing and remote collaboration tools

Instant Messaging & Social Platforms

- WhatsApp, SMS, Slack, Microsoft Teams, Telegram, Signal
- Other corporate messaging platforms
- Social media direct messaging

Automated & Integrated Channels

- AI assistants and chatbots
- API requests and responses
- Machine-triggered notifications
- Automated workflows and integration tools

Web-Based & System-Level Channels

- Company websites
- Web forms
- Digital touchpoints
- Support portals

This list is expansive but not exhaustive.

Any channel connected to, used by, or integrated into Company operations is covered by these Terms.

1.4 Entities Covered

These Terms apply to communications involving or directed to:

- **Snovasys Software Solutions Ltd (United Kingdom)**
- **Snovasys Software Solutions Pvt Ltd (India)**
- Any subsidiaries or controlled entities operating under the Snovasys group
- Any affiliates, joint ventures, or operational units
- Any brands or trademarks owned, operated, managed, or represented by the Company
- Any authorised agents, outsourced service providers, or contractors acting on behalf of the Company

Any reference to “the Company” includes all such entities collectively unless stated otherwise.

1.5 Acceptance of Terms

By communicating with the Company—through any channel, using any device, at any time—you:

- acknowledge that you have read, understood, and agreed to these Terms;
- consent to the monitoring, logging, processing, and handling of communications as described;
- agree that these Terms apply to *all* forms of interaction with the Company, even if informal, brief, or incidental;
- accept that these Terms supersede any conflicting interpretation arising from individual messages, conversations, or exchanges;
- understand that continued communication constitutes ongoing acceptance of any updated versions of these Terms.

Acceptance is **automatic and implied** through communication, regardless of whether you have explicitly accessed the Terms link.

SECTION 2 — DEFINITIONS

This Definitions section establishes the meaning of key terms used throughout this document.

Unless the context requires otherwise, all defined terms shall have the meanings set out below.

These definitions are intentionally broad, detailed, and inclusive to ensure clarity and reduce ambiguity across all jurisdictions, including the United Kingdom and the Republic of India.

2.1 "Company"

"Company" refers to **Snovasys Software Solutions Ltd**, including:

- its United Kingdom entity (including all branches, offices, and operational units),
- its Indian entity (including all subsidiaries, divisions, departments, and operational groups),
- all other affiliates, group companies, parent companies, sister companies, or joint ventures,
- all directors, officers, employees, contractors, temporary workers, consultants, advisors, interns, and authorised agents,
- any person or organisation acting on behalf of the Company with actual or apparent authority.

The term shall apply collectively and individually depending on context.

2.2 "Communication"

"Communication" includes any form of content, message, or exchange of information, whether:

- written, verbal, visual, electronic, digital, or automated;
- direct or indirect;
- synchronous (live) or asynchronous;
- formal or informal;
- intentional or unintentional.

This includes, without limitation:

- emails, text messages, instant messages, chats, posts, or comments;
- voice calls, video calls, online meetings, and recordings;
- documents, screenshots, images, files, or attachments;
- API calls, bot interactions, system responses, and automated notifications;
- metadata, logs, machine-generated messages, or system alerts.

Communication applies regardless of the platform, device, or medium used.

2.3 “Systems”

“Systems” refers to all technology and infrastructure owned, licensed, operated, or managed by or on behalf of the Company, including but not limited to:

- servers, networks, firewalls, routers, switches, and other networking components;
- cloud platforms, virtual machines, containers, and hosted environments;
- databases, data warehouses, storage systems, backup systems, and logging platforms;
- desktop and mobile applications, web applications, portals, dashboards, APIs, and admin tools;
- HRMS, CRM, communication platforms, ticketing systems, and collaboration tools;
- software, scripts, codebases, algorithms, models, and AI systems;
- internal tools, test environments, and monitoring infrastructure.

Systems include third-party tools integrated into Company operations.

2.4 “Monitoring”

“Monitoring” means any activity—automated, manual, passive, or active—involving:

- scanning,
- logging,
- analysing,
- recording,
- reviewing,
- tracking,
- intercepting,
- inspecting, or
- supervising

communications, user activity, system behaviour, or network traffic.

Monitoring includes:

- cybersecurity detection,
- compliance supervision,
- operational logging,
- fraud prevention,
- performance analysis,
- call monitoring and recording,
- audit log retention.

Monitoring may occur continuously and without explicit notice for each event.

2.5 “User”

“User” means any individual or organisation interacting with the Company, including:

- customers, clients, prospects, and leads;
- employees, contractors, and internal personnel;
- vendors, suppliers, service providers, partners, and consultants;
- website visitors, platform users, and API consumers;
- persons engaging with the Company through social media, phone, chat, email, or any other medium.

A User may act in an individual or organisational capacity.

2.6 “Recording”

“Recording” refers to the capture, storage, or reproduction of:

- audio,
- video,
- screen content,
- screensharing sessions,
- voice notes,
- transcripts,
- chat interactions,
- visual elements,
- meeting content,
- system or operational metadata.

Recordings may be created manually or automatically by Company Systems or third-party platforms.

2.7 “Metadata”

“Metadata” includes any data describing or associated with communications, interactions, devices, or system activity, including:

- timestamps, message IDs, routing paths, mail-server logs;
- IP addresses, MAC addresses, user-agent strings, device identifiers;
- login attempts, access logs, and authentication methods;
- session duration, meeting attendance, join/leave times;
- geolocation signals and network identifiers;
- performance metrics, error traces, diagnostic logs;
- API headers, payload sizes, request/response codes.

Metadata may be stored, analysed, and retained for operational, security, and compliance purposes.

2.8 “Digital Interaction”

“Digital Interaction” refers to any engagement with:

- Company websites, portals, dashboards, or user interfaces;
- mobile apps, desktop clients, extensions, or integrated tools;
- chatbots, AI assistants, automated workflows, or virtual agents;
- APIs, webhooks, SDKs, integrations, or automation pipelines;
- file uploads, form submissions, authentication flows, or system actions.

Digital Interaction includes both human-initiated and machine-initiated events.

2.9 “Applicable Law”

“Applicable Law” refers to all laws, regulations, standards, and binding obligations relevant to the Company’s operations, including:

2.9.1 United Kingdom

- UK GDPR,
- Data Protection Act 2018,
- Privacy and Electronic Communications Regulations (PECR),
- Companies Act,
- relevant regulatory guidance.

2.9.2 Republic of India

- Digital Personal Data Protection Act (DPDPA) 2023,
- Information Technology Act and Rules,
- Indian Contract Act,
- applicable regulatory guidance.

2.9.3 International Norms

Where relevant:

- cross-border transfer rules,
- telecom regulations,
- cloud and cybersecurity standards,
- applicable international privacy principles.

2.10 “Confidential Information”

“Confidential Information” includes any non-public information disclosed, transmitted, or stored in connection with the Company, including:

- business strategies, plans, pricing, and commercial terms;
- product designs, prototypes, documentation, and roadmaps;
- source code, algorithms, models, and technical architecture;
- client lists, vendor details, and partner information;
- personal data, sensitive data, and employee information;
- internal communications, recordings, logs, and operational workflows;
- security configurations, credentials, and authentication details.

Confidential Information remains confidential regardless of whether it is intentionally or inadvertently disclosed.

2.11 Additional Terms

Without limitation, the following terms are also defined for completeness:

- **“Processing”** – any operation performed on data.
- **“Personal Data”** – any information relating to an identifiable individual.
- **“Third-Party Provider”** – any external service or platform integrated into operations.
- **“Content”** – any data, communication, file, or material exchanged.
- **“Session”** – a period of interaction between a User and the System.
- **“Credentials”** – passwords, tokens, keys, or authentication materials.
- **“Service Provider”** – any contractor or vendor handling data or systems.
- **“Security Event”** – any event affecting confidentiality, integrity, or availability.
- **“Breach”** – unauthorised access, disclosure, alteration, or destruction of data.
- **“Retention”** – storage or preservation of data for operational or legal reasons.
- **“Automated Decision-Making”** – algorithmic or machine-based processing.
- **“Law Enforcement Request”** – a formal request by authorities for information.

SECTION 3 — GENERAL COMMUNICATION TERMS

This section establishes the fundamental principles governing the nature, meaning, and legal effect of communications exchanged with the Company.

Users should interpret all interactions in accordance with the disclaimers and limitations outlined below.

3.1 No Legal, Tax, Accounting, or Financial Advice

Users acknowledge and agree that:

- No communication issued by the Company—whether written, verbal, electronic, automated, or otherwise—constitutes legal, tax, accounting, financial, investment, regulatory, compliance, or other professional advice.
- Any information, comments, or guidance provided is offered solely for general informational or operational purposes and must not be interpreted as expert or specialist advice.
- Users should seek independent professional counsel before relying on any information in contexts involving:
  - legal risk,
  - regulatory compliance,
  - financial decisions,
  - accounting treatment, or
  - contractual commitments.

The Company disclaims liability for decisions made based on such communications.

3.2 No Professional Guarantees or Assurances

Users acknowledge that:

- No communication—whether by email, chat, phone, meeting, or other channel—should be construed as a guarantee of performance, outcomes, timelines, specifications, expected results, or suitability for any particular purpose.
- Statements made by employees or representatives may reflect preliminary views, operational context, or working assumptions and do not constitute formal assurances.
- Variations in real-world implementation, technical dependencies, and unforeseen events may affect outcomes.

The Company expressly disclaims any implied warranties or guarantees arising from informal or preliminary communications.

3.3 Subject to Contract

All communications related to business terms, pricing, commitments, deliverables, scope, timelines, strategies, implementation, or commercial arrangements are **non-binding** unless:

- documented in a formal written agreement,
- expressly approved by authorised Company personnel, and
- executed (signed) by both parties.

Users acknowledge that:

- informal discussions, drafts, proposals, or email exchanges do not create enforceable obligations;
- "agreement in principle" does not constitute a contract;
- any negotiation or suggestion remains subject to internal review and approval;
- final binding commitments require a fully executed contract.

This clause supersedes any contradictory implication from prior communications.

3.4 No Duty of Care Established

Users agree that:

- The mere act of communicating with the Company does not establish any fiduciary responsibility, duty of care, advisory obligation, or special relationship of trust.
- Communications are not intended to create attorney-client, consultant-client, or professional-client relationships.
- The Company is under no obligation to act in the User's best interest beyond standard legal and contractual responsibilities.
- No reliance shall be placed on the assumption that the Company is assuming such duties through casual or operational communications.

This limitation stands regardless of the tone, detail, or professionalism of the communication.

3.5 Accuracy Disclaimer

Users acknowledge that:

- Communications may occasionally contain incomplete, outdated, preliminary, or approximate information;
- Operational messages may rely on information available at the time of communication and may not reflect later developments;
- Technical descriptions, timelines, or interpretations may be representative rather than definitive;
- Errors, omissions, or misinterpretations may occur despite reasonable efforts at accuracy;
- The Company does not warrant that communications are comprehensive, perfect, or suitable for unique or specialised use-cases.

Users are responsible for independently validating critical information before acting upon it.

SECTION 4 — EMAIL TERMS

Email is one of the primary communication channels used by the Company.

Users acknowledge that email communication inherently involves operational, technical, and security limitations, and therefore must be treated accordingly.

This section outlines the Company's position regarding email transmission, confidentiality, logging, and legal effect.

4.1 Delivery Risks

Users recognise and accept that email transmission is dependent on multiple third-party systems, networks, and security layers that are outside the Company's direct control.

Accordingly, the Company does **not** guarantee uninterrupted or successful delivery of any email.

Emails may, without limitation:

- be **delayed** due to network congestion, mail server queues, or routing issues;
- be **corrupted** during transmission or storage;
- be **blocked** by spam filters, firewalls, or antivirus systems;
- be **filtered** into junk folders or security quarantine;
- be **misdirected** due to incorrect addressing or auto-complete errors;
- be **intercepted** or altered by third-party systems, ISPs, or malicious actors;
- be **duplicated** or partially delivered;
- fail to arrive entirely for reasons outside Company control.

The Company is not responsible for:

- delays in receiving or responding to emails;
- losses arising from failure to deliver or delayed delivery;
- reliance placed on emails that were altered or corrupted in transit.

Users should not rely on email for urgent, sensitive, or time-critical communications without obtaining explicit confirmation of receipt.

4.2 Confidentiality

Emails from the Company may contain confidential, privileged, or proprietary information.

If you receive an email that **is not intended for you**, you must immediately:

- refrain from reading, copying, storing, forwarding, or disseminating the email;
- notify the sender or the Company of the misdelivery;
- permanently delete the email and any attachments from all systems, backups, and devices.

The accidental transmission of an email to an unintended recipient **does not waive confidentiality, privilege, intellectual property rights, or any legal protection** attached to the contents.

Users must handle all Company emails in accordance with:

- confidentiality obligations,
- data protection laws,
- internal policies (if an employee),
- and reasonable expectations of privacy and discretion.

4.3 Metadata Logging

In the course of sending, receiving, or processing emails, the Company may automatically log, capture, or store **email metadata**, including but not limited to:

- sender and recipient details;
- timestamps of sending, receiving, and server hops;
- message size, headers, routing details, and technical identifiers;
- IP addresses and device metadata associated with transmission;
- spam, phishing, or security analysis results;
- delivery and read status (where available);
- anti-malware scanning results;
- bounce codes, relay paths, and SMTP diagnostics.

Metadata logging occurs for operational purposes such as:

- ensuring email deliverability;
- monitoring system health and performance;
- identifying abuse or security incidents;
- maintaining audit trails;
- satisfying compliance or legal requirements;
- preventing fraud, phishing, and impersonation attempts.

Users acknowledge that metadata may be processed by internal systems, third-party email providers, and automated security platforms.

4.4 Non-binding Communications

Unless expressly stated otherwise, communications sent via email:

- **do not constitute a binding agreement**,
- **do not create contractual obligations**,
- **do not represent final commitments**,

- **do not form part of any legally enforceable contract**,
- **and may not be relied upon as definitive statements of intent**.

All proposals, quotations, timelines, commercial terms, commitments, statements of work, and decisions communicated by email remain **subject to contract**, internal approval, and execution of a formal written agreement signed by authorised Company personnel.

Users acknowledge that:

- informal emails do not create legally binding obligations;
- miscommunication or ambiguity in email should not be interpreted as contractual commitment;
- final agreements must be documented separately in writing;
- verbal or emailed assurances do not override signed contractual terms.

No employee, contractor, or representative may bind the Company to a legal commitment through email unless expressly authorised and acting within the scope of that authority.

4.5 Product Updates, Webinars & Promotional Communications

The Company may, from time to time, send email communications to Users that include, without limitation:

- product updates, feature announcements, and service enhancements;
- information about new or existing offerings;
- invitations to webinars, demos, events, or training sessions;
- operational announcements or platform-related notifications;
- promotional, educational, or marketing-related content relevant to the Company's products or services.

Such communications may be sent where the User has:

- provided contact details to the Company in the course of a business relationship;
- engaged with the Company's products, services, platforms, websites, or communications; or
- otherwise interacted with the Company in a professional or commercial context.

Users acknowledge and agree that:

- receipt of such emails forms part of ordinary business communication;
- promotional or informational content does not alter the non-binding nature of email communications;
- the Company retains discretion over the frequency, format, and content of such communications.

Where required by applicable law, Users will be provided with an option to manage preferences or opt out of non-essential promotional communications.

Operational, transactional, security, or service-related emails may continue to be sent where necessary, irrespective of promotional opt-out preferences.

The Company does not guarantee delivery, receipt, or visibility of any such communications, which remain subject to the delivery risks and limitations described in this Section.

SECTION 5 — PHONE CALLS, VIDEO CALLS & ONLINE MEETINGS

The Company conducts business through various communication channels, including telephone calls, video conferences, online meetings, virtual collaboration tools, and screensharing sessions.

Users acknowledge that participation in such communications may involve monitoring, logging, recording, or system-level metadata collection necessary for operational integrity, security, and quality.

5.1 Call Monitoring & Recording

Users acknowledge and expressly consent to the possibility that **telephone calls, VoIP calls, video calls, and online meetings may be monitored or recorded**, in whole or in part, by the Company or its authorised representatives for legitimate and routine business purposes, including but not limited to:

5.1.1 Compliance & Regulatory Requirements

- Ensuring adherence to internal policies
- Demonstrating compliance with legal or contractual obligations
- Satisfying audit requirements
- Supporting investigations into misconduct or disputes

5.1.2 Training & Quality Assurance

- Improving communication standards
- Providing training material for staff
- Enhancing service quality

5.1.3 Security & Threat Detection

- Identifying suspicious or malicious behaviour
- Verifying authenticity of participants
- Protecting against fraud, impersonation, or social engineering attempts

5.1.4 Dispute Resolution & Evidence Preservation

- Establishing factual context for conversations
- Supporting resolution of disagreements or claims
- Documenting interactions when complaints arise

5.1.5 Operational Continuity & Record-Keeping

- Maintaining reliable operational logs
- Retaining event histories where appropriate
- Supporting business continuity processes

Recordings may capture:

- audio,
- video,
- participant identifiers,
- timestamps,
- meeting names,
- shared content,
- and other associated metadata.

Not all calls are recorded, and lack of recording does not imply negligence, concealment, or wrongdoing.

5.2 Screensharing Supervision

During video calls or virtual meetings where screensharing is enabled, Users acknowledge and agree that:

- Any content displayed on-screen may be viewed by Company personnel;
- Screensharing events may generate system or platform logs noting when sharing began or ended;
- Screenshared sessions may be recorded if the meeting itself is recorded;
- Screensharing may be monitored for compliance, training, or operational needs;
- The Company does not assume responsibility for protecting on-screen data that the User voluntarily chooses to share.

Users must exercise discretion and ensure they do not unintentionally display confidential, sensitive, or inappropriate material.

5.3 Meeting Metadata Collection

Users acknowledge that modern conferencing systems inherently collect and transmit metadata, which may be logged or stored by the Company or third-party meeting providers.

Metadata may include, without limitation:

- meeting join and leave times;
- meeting duration;
- participant names or identifiers;
- email addresses or login information;
- IP addresses, geolocation approximations, or network identifiers;
- device identifiers, OS and browser type, version information;
- bandwidth or network performance metrics;
- call quality data such as latency, jitter, packet loss, and stability indicators;
- meeting title, ID, host details, and platform-level session logs.

This metadata may be used for:

- diagnosing technical issues,
- analysing meeting stability,
- ensuring system security,
- confirming attendance,
- supporting compliance and dispute-resolution processes.

The Company does not control what metadata is inherently collected by third-party conferencing platforms, which operate under their own policies.

5.4 Responsibility for User Environment

Users bear full responsibility for managing and securing their own physical and digital environments during calls, meetings, or screensharing sessions. This includes:

- ensuring confidential documents or screens are not visible unintentionally;
- managing background visibility and audio capture;
- preventing unauthorised individuals from overhearing or viewing sensitive discussions;
- ensuring devices used for calls are secure, updated, and malware-free;
- disabling notifications or pop-ups that may reveal personal or confidential information;
- avoiding the sharing of sensitive materials unless absolutely necessary.

The Company is not responsible for any disclosure, reputation impact, or loss arising from User negligence, carelessness, or oversight during participation in calls or online meetings.

SECTION 6 — ELECTRONIC COMMUNICATION CHANNELS

The Company utilises multiple electronic communication channels to support operations, coordination, collaboration, and service delivery.

Users acknowledge that all interactions across these channels may be processed, logged, analysed, retained, monitored, or reviewed in accordance with these Terms, applicable law, and operational requirements.

6.1 Instant Messaging Channels

The Company may communicate or receive communications through various instant messaging platforms, including but not limited to **WhatsApp, SMS, Slack, Microsoft Teams, Telegram, Signal, iMessage**, and other business messaging services.

Users acknowledge and agree that:

- **Metadata and message information** exchanged through these channels may be logged, including timestamps, participants, message status, device identifiers, and connection details.
- Messages may be captured for:
  - operational coordination,
  - troubleshooting,
  - dispute resolution,

  - compliance reviews,
  - security monitoring, and
  - quality assurance.
- Certain instant messaging platforms inherently store messages on third-party servers; the Company has limited or no control over those storage and processing practices.
- Messaging channels may integrate with Company Systems (e.g., for notifications, ticketing, automation, or alerts).
- Content sent to or received from the Company through instant messaging may be incorporated into:
  - customer support workflows,
  - CRM records,
  - audit trails,
  - documentation repositories.
- The Company may retain or archive message history for operational or compliance purposes where permitted.
- Voice notes, attachments, photos, links, or other file types shared via messaging platforms may be scanned or processed for malware detection, quality assurance, or record-keeping.

Users must not transmit confidential, sensitive, or restricted content through instant messaging unless specifically authorised and protected through appropriate channels.

6.2 Chatbots, Virtual Assistants & AI Interfaces

The Company may utilise automated chatbots, virtual assistants, AI-driven communication tools, intelligent support agents, or machine-learning interfaces to facilitate communication, answer queries, assist with troubleshooting, or streamline workflows.

Users acknowledge and agree that:

- Interactions with automated systems may be **logged, analysed, processed, or evaluated** to improve system performance, accuracy, safety, and compliance.
- Data may be reviewed to refine AI models, correct errors, enhance user experience, identify misuse, or adapt conversational responses.
- Interactions may be monitored to detect:
  - abnormal behaviour,
  - security threats,
  - malicious attempts to manipulate AI behaviour,
  - spam, fraud, or adversarial inputs.
- AI systems may use aggregated or anonymised data for:
  - quality improvement,
  - operational analytics,
  - system training or optimisation.
- Responses generated by AI systems should not be construed as:
  - legal advice,
  - financial advice,
  - technical guarantees,
  - or binding commitments.

Users must not attempt to exploit, reverse-engineer, manipulate, or compromise AI behaviours, including prompting the system to reveal internal logic, proprietary information, or sensitive data.

6.3 Social Media Direct Messaging & Online Interactions

The Company may engage with Users through direct messaging features available on social media platforms such as **LinkedIn, Facebook, Instagram, Twitter, YouTube, and others**.

Users acknowledge that:

- Social media platforms inherently capture and store metadata, which is outside the Company's control.
- Direct messages sent to the Company through social channels are subject to these Terms, including monitoring, retention, logging, and compliance mechanisms.
- Responses through social media may be limited, automated, or handled by third-party tools or social media integrations.
- Communications received via social media may be transferred into internal systems (e.g., CRM, support tools) for operational handling.
- Users must not rely on social media communication for urgent, confidential, or sensitive matters.
- Communication through social media does **not** constitute formal notice to the Company unless explicitly stated.

Users must use such platforms responsibly and must not transmit sensitive, confidential, or proprietary information via social media unless explicitly authorised and secure methods have been agreed.

SECTION 7 — ACCEPTABLE USE POLICY

The Company's communication channels, systems, infrastructure, networks, platforms, tools, and digital resources ("Company Systems") are provided for legitimate, authorised, and lawful business purposes.

Users agree to comply with the following Acceptable Use Policy, which defines prohibited behaviours, misuse scenarios, and actions that may result in suspension, restriction, investigation, or legal enforcement.

7.1 Prohibited Uses

Users shall **not**, under any circumstances, use Company Systems — directly, indirectly, intentionally, unintentionally, manually, or by automation — to engage in any of the activities listed below.

These prohibitions apply to all communication channels, including email, calls, chat, APIs, platforms, integrations, and automated systems.

7.1.1 Unlawful, Harmful, or Fraudulent Activities

Users may not:

- engage in illegal, deceptive, fraudulent, or harmful acts;
- transmit or support activities related to identity theft, data theft, piracy, scams, or financial fraud;
- violate any applicable law, regulation, or contractual obligation;
- engage in behaviour that exposes the Company to legal or regulatory risk.

7.1.2 Attacks, Breaches, Scanning & Probing

Users may not:

- attempt to hack, breach, circumvent, or compromise security measures;
- scan or probe networks, ports, endpoints, APIs, or infrastructure;
- perform penetration testing or ethical hacking without **explicit written permission**;
- use tools or scripts to analyse system vulnerabilities;
- attempt to gain unauthorised access to accounts, systems, or data.

7.1.3 Dissemination of Malware or Malicious Content

Users may not:

- upload, transmit, or distribute viruses, trojans, ransomware, spyware, or any malicious code;
- send harmful links or attachments designed to compromise devices or accounts;
- deliberately degrade system performance or availability.

7.1.4 Harassment, Abuse, or Misconduct

Users may not:

- harass, bully, intimidate, threaten, or abuse Company staff or other users;
- engage in hostile, inappropriate, discriminatory, or offensive communications;
- use communications to cause distress, reputational harm, or workplace disruption.

7.1.5 Impersonation & Misrepresentation

Users may not:

- impersonate any person, employee, representative, or system identity;
- forge headers, metadata, signatures, or email origins;
- misrepresent authority, affiliation, or identity in any communication.

7.1.6 Uploading Harmful, Unauthorized, or Inappropriate Files

Users may not:

- upload corrupted files, dangerous executables, or unapproved scripts;
- transfer proprietary or confidential information without authorisation;
- upload content that violates intellectual property rights, privacy, or security rules.

7.1.7 Sharing Confidential Information Without Authority

Users may not:

- transmit confidential, internal, personal, or proprietary Company information without permission;
- forward restricted content to unauthorised third parties;
- expose sensitive operational or commercial data via any channel.

7.1.8 Privilege Escalation Attempts

Users may not:

- attempt to obtain elevated permissions, admin access, or system control through improper means;
- manipulate roles or privileges within Company Systems;
- bypass or tamper with authentication, authorisation, or access control mechanisms.

7.1.9 Interference with Service Operations

Users may not:

- disrupt, overload, degrade, or interfere with system operations or communications;
- cause denial-of-service conditions;
- automate excessive requests beyond acceptable usage;
- intentionally create performance issues or outages.

7.1.10 Competitive Intelligence, Scraping & Harvesting

Users may not:

- scrape, harvest, or extract data, content, or metadata from Company Systems for competitive analysis;
- use bots, crawlers, or automation tools to collect information without written permission;
- reverse-engineer Company intellectual property or reproduce proprietary features.

7.1.11 Reverse Engineering, Decompiling & Code Analysis

Users may not:

- reverse-engineer, decompile, or disassemble software, tools, or platforms;
- inspect underlying code, logic, models, or algorithms;
- analyse system behaviour to replicate functionality or derive confidential information.

7.1.12 Circumventing Security Protocols

Users may not:

- disable or evade security features, monitoring systems, or restrictions;
- manipulate device or network configurations to hide identity or avoid detection;
- use VPNs, proxy chains, anonymity tools, or spoofing techniques to bypass controls.

7.1.13 Sending Spam, Mass Messaging, or Unauthorized Broadcasts

Users may not:

- send spam, junk mail, phishing content, mass unsolicited communications, or advertisements;
- conduct bulk messaging campaigns without explicit authorisation;
- misuse communication channels for promotional or non-business activity.

7.1.14 Other Prohibited Conduct

Users may not engage in any behaviour that:

- threatens system stability or security,
- misuses communication channels for non-legitimate purposes,
- violates rights of any third party,
- exposes the Company to legal, operational, or reputational harm,
- contradicts any law, regulation, or these Terms.

7.2 System Abuse & Enforcement Actions

The Company reserves the right to take immediate and proportionate action when misuse, suspicious behaviour, or violation of this Acceptable Use Policy is detected or reasonably suspected.

Such actions may include, without limitation:

- **temporary suspension** of communication channels;
- **permanent restriction** of system access;
- **throttling or blocking** of traffic or accounts;
- **revocation** of access credentials, API keys, or privileges;
- **manual or automated investigations** of user activity;

- **forensic analysis** of logs, device fingerprints, or communication metadata;
- **notification to legal authorities** where required;
- **reporting** to external regulators or partners;
- **termination** of business relationships in severe cases.

Users acknowledge that enforcement measures may occur without prior notice if immediate action is necessary to protect system integrity, legal compliance, or operational stability.

SECTION 8 — IT SECURITY, THREAT DETECTION & SURVEILLANCE

The Company maintains sophisticated, multi-layered security, monitoring, and threat-detection frameworks designed to protect its systems, users, infrastructure, data, and communication channels.

Users acknowledge that these security processes operate continuously, automatically, and without manual intervention, and form a core part of lawful and responsible system operation.

8.1 Automated Security Monitoring

The Company employs **automated, intelligent, and adaptive security monitoring technologies** across its digital infrastructure. These systems may continuously collect, analyse, process, and evaluate data to ensure integrity, detect anomalies, and prevent harm.

Automated monitoring may include, without limitation:

8.1.1 Intrusion Detection Systems (IDS)

Systems may detect unusual traffic, unauthorised access attempts, exploitation signatures, or suspicious network behaviour.

8.1.2 Firewall Logging

Ingress, egress, and internal network requests may be logged and evaluated for rule violations, anomalies, or malicious activity.

8.1.3 Behavioural Analytics

Machine-learning and pattern-recognition systems may analyse typical and atypical user behaviour to detect:

- deviations from normal usage,
- compromised accounts,

- insider threats,
- automation abuse,
- data exfiltration attempts.

8.1.4 Session Tracing

Session metadata—including IP addresses, device properties, duration, actions taken, and transitions—may be tracked to ensure authenticity and security.

8.1.5 Threat Scoring & Risk Assessment

Systems may assign threat scores to events or sessions based on known attack patterns or anomalies.

8.1.6 Bot Detection

Traffic may be analysed to identify automated scripts, crawlers, hostile bots, or unusual automation behaviour.

8.1.7 Phishing Detection

Inbound and outbound communications may be scanned for phishing indicators, spoofing, impersonation, or malicious payloads.

8.1.8 Malware Scanning

Attachments, uploads, downloads, and files exchanged through Company systems may be scanned for viruses, trojans, ransomware, or other malicious code.

8.1.9 Endpoint & Client Signals

Device-level signals may include:

- operating system details,
- browser fingerprints,
- configuration characteristics,
- security status,
- hardware identifiers.

These signals assist in detecting unsafe or compromised devices.

8.1.10 API Monitoring

API activity may be logged and analysed for:

- abuse patterns,
- unusual request volumes,
- credential misuse,
- unauthorised access attempts.

8.1.11 Authentication & Failed Login Analysis

Failed login attempts, password resets, unusual login locations, or suspicious authentication flow behaviour may be analysed to detect attacks or compromised accounts.

Users explicitly acknowledge that all such monitoring is **routine, automated, and necessary** for system security.

8.2 Network Surveillance

The Company may conduct **passive and active network analysis** within its systems and infrastructure.

This analysis may review or capture network metadata relating to:

- **Threat identification:** detecting attacks, intrusions, lateral movement, or malicious activity.
- **Misuse and policy violations:** identifying unauthorised or inappropriate use of communication channels.
- **Performance monitoring:** analysing slowdowns, packet loss, routing issues, or congestion.
- **Suspicious behaviour:** detecting anomalies such as unusual data volumes, unexpected destinations, or suspicious payloads.
- **Abuse pattern analysis:** detecting repeated violations, brute-force attempts, scraping, or credential stuffing.

Network surveillance is executed strictly for security, operational continuity, and compliance purposes.

8.3 Device Fingerprinting

To protect against fraud, impersonation, and system compromise, the Company may capture **device fingerprinting data**, including but not limited to:

- device type and characteristics,
- hardware identifiers (where available),
- OS version and patch levels,
- browser type, version, settings, and plugins,
- language and timezone settings,

- network identifiers (e.g., IP, ASN),
- unique or semi-unique device signatures.

Device fingerprinting enables:

- detection of unusual device changes,
- surveillance of multi-account misuse,
- prevention of credential sharing or impersonation,
- strengthening of authentication and access control mechanisms.

Such fingerprinting is standard practice in enterprise systems.

8.4 Automated Alerts & Escalations

Upon detecting suspicious, anomalous, or high-risk behaviour, the Company's systems may automatically:

- generate internal alerts,
- escalate notifications to IT or security personnel,
- temporarily restrict access,
- block high-risk actions,
- force re-authentication,
- throttle or suspend suspicious sessions,
- trigger deeper security analysis.

These responses occur without user notification where appropriate, and are essential for safeguarding infrastructure.

8.5 Lawful Basis for Monitoring & Surveillance

Users acknowledge that monitoring, logging, and surveillance conducted under this Section is performed based on the following lawful bases:

8.5.1 Legitimate Interests (UK GDPR)

Monitoring is necessary for:

- security of systems and data,
- fraud prevention,
- safeguarding operational infrastructure,
- complying with company policies,
- detecting misuse or violations,
- maintaining communication integrity.

8.5.2 Compliance with Applicable Laws (UK & India)

Monitoring may be carried out to:

- comply with legal obligations,
- retain evidence for disputes,
- maintain audit and accountability records.

8.5.3 Business Necessity

Monitoring is essential for operating a secure, functional, and reliable communication environment.

8.5.4 Routine IT & Cybersecurity Operations

All monitoring is carried out as **standard industry practice** and is not targeted at any individual unless required for investigation or compliance.

SECTION 9 — SYSTEM LOGGING & AUDIT TRAILS

9.1 Categories of Logs Captured

The Company employs comprehensive logging and audit mechanisms across its systems, platforms, communication channels, and infrastructure.

These logs are essential for maintaining operational stability, ensuring security, diagnosing issues, and meeting compliance standards.

Users acknowledge and agree that the Company may capture, generate, or store logs including, but not limited to, the following categories:

9.1.1 Email Logs

- Message routing details
- Sender and recipient information
- Timestamps
- Delivery status and bounce information
- Spam-filtering and security analysis metadata

9.1.2 Call Logs

- Caller and callee identifiers
- Call duration
- Join/leave times

- Quality metrics (e.g., jitter, packet loss)
- Device and connection details
- Conference platform metadata

9.1.3 Chat Logs

- Messages exchanged over instant messaging channels
- Ticketing system communications
- In-app chat interactions
- Chatbot conversation metadata
- User-to-agent transcripts where applicable

9.1.4 System Access Logs

- Login attempts (successful and failed)
- Authentication method used
- Access time stamps
- IP addresses and geolocation estimates
- Device/browser identifiers
- Session token usage and expiration

9.1.5 Error Logs

- Application error traces
- System fault messages
- Crashes, exceptions, and warnings
- Platform-level failure indicators
- Infrastructure error reporting

9.1.6 Application Event Logs

- User activity events
- Workflow execution logs
- API calls and responses
- Feature usage patterns
- Performance metrics

9.1.7 User Action Logs

- Button clicks, navigation paths
- Configuration or settings changes
- File uploads or downloads
- Administrative or privileged operations
- Data modification records

9.1.8 Authentication Logs

- Multi-factor authentication events
- Password changes and resets
- Access token creation and revocation
- Role-based access control triggers

9.1.9 Security Events

- Firewall and intrusion detection system alerts
- Suspicious behaviour patterns
- Malware or phishing detections
- Blocked access attempts
- Privilege escalation attempts
- Compliance rule violations

Users acknowledge that such logging is **standard industry practice** and may involve automated tools, AI-driven analysis, and third-party security platforms.

9.2 Existence of Logs

Users acknowledge that:

- logs are created automatically as part of routine operations;
- the Company is **not obligated** to maintain any particular log, record, or audit trail unless explicitly required to do so under applicable law, regulation, or contractual obligation;
- logs may be stored, rotated, overwritten, compressed, aggregated, anonymised, archived, or deleted at the Company's discretion as part of system maintenance or retention schedules;
- not all logs are retained permanently, and some logs may exist only transiently due to system architecture, storage tiers, or security policies;
- absence of a log does not imply negligence, deletion, tampering, concealment, or wrongdoing by the Company.

Users explicitly agree that logging practices may evolve over time due to technology updates, security improvements, or infrastructure changes.

9.3 Use of Logs

Logs may be accessed, analysed, reviewed, processed, or otherwise utilised by the Company or authorised personnel for legitimate purposes, including but not limited to:

9.3.1 Abuse Detection & Prevention

- detecting unauthorised or malicious activity,
- identifying system misuse,
- enforcing acceptable use policies,
- monitoring violation patterns.

9.3.2 Dispute Resolution

- clarifying events leading to disagreements,
- reconstructing timelines,
- resolving inconsistencies in communication or behaviour,
- evidentiary support in investigations.

9.3.3 Fraud Prevention

- identifying suspicious activities,
- preventing fraudulent transactions or impersonation,
- tracing anomalous sequences or automation abuse.

9.3.4 Security Incidents

- analysing attempted breaches or intrusions,
- tracing compromised accounts or devices,
- reviewing events leading to system threats.

9.3.5 System Failures & Diagnostics

- troubleshooting performance degradation,
- resolving bugs or operational defects,
- identifying root causes of outages or malfunctions,
- improving system stability and reliability.

Logs may be retained or reviewed by internal IT teams, compliance teams, security personnel, or authorised third-party service providers operating under confidentiality obligations.

SECTION 10 — DATA RETENTION, ROTATION & AUTOMATED DELETION

10.1 Automated Retention Schedules

The Company maintains **structured, automated data retention schedules** designed to ensure operational efficiency, compliance with applicable laws, and responsible data governance practices.

Users acknowledge and agree that:

- different categories of data (such as communications, metadata, logs, recordings, ticket history, and system-generated events) may be retained for **varying durations**;
- retention periods may be determined by operational necessity, fraud prevention requirements, audit policies, contractual obligations, legal mandates, or technical constraints;
- automated tools may classify and retain data according to internal rules, policies, industry standards, or system-defined service logic;
- retention practices may vary across environments, geographies, systems, or communication channels.

Nothing in these Terms obligates the Company to maintain any specific category of data for any specific period unless expressly required by law or contract.

10.2 Automated Deletion Processes

Users acknowledge that the Company employs **automated deletion mechanisms**, which may periodically remove older or unnecessary data without manual intervention.

Such automated deletions may occur due to:

- **Storage optimisation:** Ensuring system performance, reducing unnecessary storage utilisation, and maintaining efficient data architecture.
- **Retention schedules:** Automatically removing data upon expiration of predefined time periods.
- **Compliance policies:** Ensuring conformity with legal, regulatory, industry, or internal governance requirements.
- **System maintenance:** Routine or event-based cleanup tasks executed as part of infrastructure management.
- **Technical constraints:** Storage tiering, log rotation, index rebuilding, or platform-imposed data lifecycles.

Automated deletion may include, but is not limited to:

- call recordings,
- email logs,
- video meeting metadata,
- chat transcripts,
- access logs,
- system error logs,
- browser session data,
- archival files,
- expired snapshots, or

- redundant backups.

Users explicitly acknowledge that **automated deletion is a normal, standard operational function** and occurs continuously as part of system hygiene.

10.3 Non-Association Disclaimer

To avoid any misunderstanding, allegation, or adverse inference, Users acknowledge that:

- The execution of automated deletion processes is **routine**, **neutral**, and **policy-driven**.
- Automated deletions are **not triggered by**, **in response to**, or **associated with** any specific:
    - dispute,
    - complaint,
    - allegation,
    - investigation,
    - employee action,
    - legal threat,
    - customer escalation,
    - regulatory concern, or
    - interpersonal conflict.

These processes continue irrespective of any individual communication or issue.

The Company expressly disclaims any suggestion that the absence, deletion, modification, rotation, overwriting, or non-availability of data implies wrongdoing, evidence tampering, concealment, or any adverse intent.

Such deletions occur **solely due to automated system operations**, standard IT maintenance, or established retention policies.

10.4 Archival & System Snapshots

For continuity, resilience, and disaster recovery purposes, the Company may maintain **periodic archival copies, backups, or system snapshots**.

Users acknowledge that:

- backups are intended solely for operational recovery, not long-term storage of communications;
- archived data may not be accessible for general retrieval or user requests;
- backup storage may occur across distributed or multi-region infrastructure;
- archived data may be overwritten as part of rolling backup cycles;

- snapshots may not preserve communications in real time and may not include every item.

The presence of an archive or backup does not guarantee retrieval, recovery, or availability of any particular communication, log, or data element.

The Company may restore data from backups only when necessary for operational continuity or security, and not for reconstructing communication histories outside legitimate technical purposes.

SECTION 11 — PRIVACY & DATA PROCESSING

11.1 UK GDPR Compliance

To the extent that personal data is processed in connection with communications, system interactions, or operational activities within the **United Kingdom**, such processing shall be carried out in accordance with the requirements of the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and any applicable guidance issued by the Information Commissioner's Office (ICO).

This includes, where applicable:

- maintaining lawful bases for processing personal data;
- ensuring transparency in data-handling practices;
- applying appropriate technical and organisational security measures;
- limiting data collection to what is necessary for operational, security, or monitoring purposes;
- retaining data only for lawful and proportionate durations;
- implementing safeguarding measures for international transfers;
- ensuring that third-party processors meet required data protection standards.

Users acknowledge that communications may inherently involve the processing of personal data, including metadata, identifiers, contact details, behavioural signals, and operational information necessary to facilitate communication and maintain system integrity.

11.2 India DPDPA Compliance

To the extent that personal data is processed within or connected to the Company's operations in **India**, such processing shall be undertaken in alignment with the principles and obligations established under the **Digital Personal Data Protection Act, 2023 (DPDPA)** and relevant implementing rules.

This includes:

- adherence to purpose limitation and data minimisation;
- maintaining reasonable security safeguards;
- complying with lawful processing principles;
- ensuring that personal data is processed only for legitimate business, operational, and compliance-related purposes;
- respecting data principal rights insofar as they do not conflict with compliance obligations, contract enforcement, or legitimate business interests;
- ensuring processors handling data on behalf of the Company maintain appropriate security and privacy controls.

Users acknowledge that communications inherently involve the flow of operational and personal data, which may be required for fraud prevention, audit trails, IT security, monitoring, and maintaining service quality.

11.3 Cross-Border Transfer of Data

Users acknowledge and consent to the fact that communications, metadata, and operational information may be transmitted, routed, stored, processed, or mirrored across multiple jurisdictions, including but not limited to:

- the United Kingdom,
- the Republic of India,
- data centres operated by global cloud providers,
- regions where third-party tools or communication platforms are hosted.

Cross-border transfers may occur due to:

- routing of internet traffic through international networks;
- use of global cloud infrastructures (e.g., AWS, Azure, Google Cloud);
- email and messaging platform design;
- multi-region redundancy and failover systems;
- third-party providers' operational architectures.

Where required, appropriate transfer mechanisms such as contractual clauses, security measures, or certifications may be applied.

Users expressly agree that such transfers are inherent to modern communication systems and are necessary for the Company's global operations, continuity, and security.

11.4 Legitimate Interests

The Company relies on **legitimate interests** as one of the lawful bases for processing personal data, particularly in relation to:

- monitoring communication channels for compliance, security, and operational quality;
- logging access, authentication, usage, and behavioural patterns to detect misuse or threats;
- protecting the integrity of systems, data, and infrastructure;
- ensuring accurate record-keeping for audit, dispute resolution, and quality assurance;
- facilitating troubleshooting, protection against abuse, and maintenance of service reliability;
- enabling internal governance, accountability, and documentation.

Such processing is carried out in a manner that is proportionate, necessary, and aligned with both organisational obligations and user expectations in a corporate environment.

Users acknowledge that monitoring and logging activities form part of the Company's routine IT, security, and operational practices.

11.5 Exercise of Rights

Where Users are entitled to exercise data protection rights under applicable laws (e.g., access, correction, deletion, objection), such requests shall be processed in accordance with relevant legal frameworks (UK GDPR, DPDPA), subject to limitations arising from:

- security requirements,
- fraud prevention measures,
- regulatory compliance obligations,
- audit and logging necessities,
- contractual commitments,
- operational continuity,
- legitimate interests of the Company.

In certain contexts—especially in corporate, security-sensitive, or compliance-driven environments—the Company may decline or restrict certain rights requests, including those that would:

- compromise monitoring systems,
- undermine security safeguards,
- disrupt business operations,
- violate legal obligations to retain specific data,
- interfere with audits, investigations, or dispute resolution,
- expose confidential, privileged, or proprietary information.

Users acknowledge that such limitations are necessary to maintain security, integrity, and operational reliability and are consistent with global data protection norms.

SECTION 12 — THIRD-PARTY SERVICES DISCLAIMER

12.1 Use of Third-Party Tools, Platforms & Service Providers

Users acknowledge and agree that the Company's communication channels, systems, and operations may rely upon, integrate with, or be supported by a wide range of third-party providers, including but not limited to:

- **Productivity & communication suites:**

  Microsoft 365, Google Workspace, Slack, Teams, Zoom

- **Cloud hosting & infrastructure providers:**

  Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform

- **Telecommunication & network operators:**

  Internet service providers, telecom carriers, VoIP platforms, SMS gateways

- **Collaboration & meeting tools:**

  Webex, GoToMeeting, Meet, other conferencing tools

- **AI, automation, and analytics systems:**

  Machine-learning engines, chat assistants, data processing services

- **Email and messaging providers:**

  SMTP services, spam filters, routing systems, delivery networks

- **Storage, backup, and archiving technologies:**

  Object storage, CDN services, audit-log repositories

Users understand that these third-party systems may process communications, metadata, files, and interaction logs as part of their operational function. The Company does not control the internal operations, decision-making, policies, architectures, security controls, or data handling practices of such third-party providers.

Use of third-party tools may include:

- routing communications through external infrastructure
- temporary or permanent storage of metadata or content
- automated filtering, scanning, spam detection, or threat analysis

- cross-border transmission of data
- profiling or logging by the provider to support reliability and security
- execution of software or scripts within the provider's environment

Users agree that the Company may select, replace, or modify its third-party providers at any time as part of normal operational changes.

12.2 Disclaimer of Liability for Third-Party Systems

To the fullest extent permitted by applicable law, the Company disclaims all responsibility and liability for:

- downtime, outages, interruptions, or unavailability of third-party services;
- delays, delivery failures, corruption, or loss of communications arising from third-party systems;
- security vulnerabilities, breaches, or incidents within third-party infrastructure;
- policy changes, technical changes, data-storage practices, or operational failures of third-party providers;
- actions or inactions of telecom companies, cloud platforms, hosting providers, carriers, or communication intermediaries;
- failures caused by provider maintenance, upgrades, or disruptions;
- data processing practices, retention policies, or compliance posture of third-party providers;
- any limitation, defect, bug, misconfiguration, or performance issue originating outside Company-controlled environments.

Users acknowledge that third-party services operate independently and may:

- modify their terms,
- introduce changes to their functionality,
- experience service interruptions,
- enforce security or access restrictions,
- impose throughput or rate limits,
- undergo outages or maintenance,
- or terminate features without notice.

Such events are outside the Company's reasonable control and therefore **do not create liability**, nor do they constitute a breach of these Terms by the Company.

12.3 No Guarantee of Availability or Performance

The Company does not guarantee:

- uninterrupted access to communications,

- availability of any specific feature or tool,
- stability of connectivity,
- continuity of service from third-party providers,
- error-free operation of dependent technologies.

The User's sole remedy in relation to third-party failures is to cease communications or discontinue use of Company services.

SECTION 13 — TECHNOLOGY & PLATFORM INTERFACES

13.1 API Interactions

When interacting with the Company through APIs, integrations, data endpoints, or any automated programmatic interface, Users acknowledge and agree that:

- **API requests, responses, payloads, metadata, timestamps, headers, error codes, authentication events, and system behaviours may be logged, monitored, and analysed** for operational, performance, diagnostic, compliance, and security purposes.
- The Company may collect and store metadata such as IP addresses, service identifiers, user-agent strings, origin applications, token usage, rate-limit events, and access patterns.
- Logging may be conducted through internal tools, third-party monitoring systems, or cloud provider instrumentation.
- The Company may analyse API usage to detect abnormal patterns, suspicious behaviour, misuse, automation abuse, policy violations, or activities that pose security risks.
- API access may be rate-limited, throttled, temporarily suspended, or permanently restricted based on behaviour or system health requirements.
- The Company may introduce versioning, deprecate older API endpoints, or adjust throttling rules without prior notice.

Users remain fully responsible for securing their API credentials, ensuring proper authentication, and complying with API usage guidelines.

13.2 Automation & Bots

Users acknowledge that certain features, tools, or channels of communication may be powered by:

- automated scripts,
- bots,
- artificial intelligence systems,
- machine-learning models,
- workflow automation engines,

- natural language processing modules, or
- rule-based logic.

Users agree that:

- Automated tools may process, interpret, transform, or act upon User input to facilitate service delivery.
- Interactions with automated systems may be monitored or logged for accuracy, training, fraud prevention, and operational improvement.
- Automated responses may not always reflect human judgment, and Users must not rely upon such responses as legal, financial, or professional advice.
- The Company may refine, retrain, or adjust automated systems using aggregated or anonymised interaction data.
- The Company retains full discretion to modify, enhance, disable, or reconfigure automation tools at any time.

Users must refrain from manipulating automated systems or attempting to exploit bots through adversarial inputs, reverse-engineering, testing constraints, or automated probing.

13.3 Feature Evolution

Users understand and agree that:

- The Company's systems, products, features, software interfaces, tools, and communication mechanisms are **dynamic** and may evolve over time.
- As part of ongoing innovation, improvement, security strengthening, and product development, the Company may:
  - add, modify, or remove features;
  - upgrade system components;
  - alter workflows and interface designs;
  - discontinue legacy functionalities;
  - migrate to different technology platforms;
  - introduce new capabilities;
  - conduct performance optimisations;
  - adjust backend or frontend behaviour;
  - perform maintenance and updates.
- Such changes may occur **with or without prior notice**, and may temporarily or permanently affect how Users access or interact with Company systems.
- Users are responsible for adapting their usage, integrations, or dependencies to align with updated features or system behaviours.

The Company does not guarantee backward compatibility unless explicitly stated in a separate agreement.

Users relying on long-term integrations or custom workflows must independently maintain compatibility.

SECTION 14 — INTELLECTUAL PROPERTY RIGHTS

14.1 Ownership of Intellectual Property

All intellectual property rights in and to:

- all communications sent by the Company,
- all documents, files, presentations, reports, diagrams, charts, or materials shared,
- all text, images, audio, video, graphics, recordings, data, metadata, or digital assets,
- all software, code, scripts, APIs, dashboards, interfaces, and user experiences,
- all documentation, guides, manuals, and training materials,
- all proprietary models, algorithms, workflows, and processes,
- all trademarks, logos, service marks, trade names, and brand identities,
- all system designs, layouts, schemas, and architecture diagrams,
- all business logic, strategies, and frameworks,
- all content generated by or through Company systems, tools, or automation,
- all content created by employees, contractors, or authorised personnel in the course of their duties,
- all derivative works or enhancements produced in connection with Company deliverables,

are and shall remain the **exclusive property of the Company** or its licensors, regardless of whether such content is explicitly marked as proprietary.

No transfer, assignment, licence, right of use, or other ownership interest is granted to any User unless expressly provided in a separate written agreement signed by an authorised officer of the Company.

Users acknowledge that communications may contain confidential or proprietary information protected under intellectual property, copyright, trademark, and trade secret laws across multiple jurisdictions.

14.2 Restrictions on Use, Distribution, and Replication

Users are strictly prohibited from engaging in any activity that infringes upon or improperly exploits the Company’s intellectual property. This includes, without limitation:

14.2.1 Redistribution & Republishing

Users may not:

- distribute, share, republish, or circulate Company materials,
- upload Company content to public platforms, repositories, or forums,
- provide access to Company content to unauthorised third parties,
- include Company-owned materials in commercial or public deliverables.

14.2.2 Reproduction & Duplication

Users may not:

- copy, duplicate, or reproduce Company content in whole or in part,
- store or archive Company content for purposes beyond the intended scope of communication,
- integrate Company materials into external documents or presentations without authorisation.

14.2.3 Modification & Derivative Works

Users may not:

- alter, edit, modify, translate, or create derivative works based on Company content,
- adapt Company materials for use in competitive or commercial contexts,
- integrate Company content into technology, software, or tools not approved by the Company.

14.2.4 Reverse Engineering & Decompilation

Users may not:

- reverse-engineer, decompile, disassemble, or analyse the underlying structure of Company software, systems, or tools,
- attempt to extract source code, logic, models, or algorithms,
- probe or inspect system behaviour to replicate functionality.

14.2.5 Competitive Use Restrictions

Users may not:

- use any Company content to build or assist in building competing products or services,
- use insights derived from Company systems to inform competitive intelligence,
- benchmark Company proprietary technology against competitors without permission.

14.3 Limited License for Intended Use

Where content is shared in the context of business communication, the User is granted a **limited, non-exclusive, revocable, non-transferable licence** to use such content **solely for the purpose and duration of the specific communication or transaction**.

This licence does **not** extend to any form of:

- reuse,
- redistribution,
- publication,
- integration into other works, or
- long-term storage.

Any usage outside the intended scope constitutes a material breach of these Terms.

14.4 Reservation of Rights

All rights not expressly granted herein are reserved.

No implied licences or rights arise by virtue of receiving communications or interacting with Company systems.

The Company retains full rights to pursue legal remedies for any infringement.

14.5 Survival of Intellectual Property Rights

All intellectual property rights and restrictions detailed in this Section shall survive:

- termination of communication,
- cessation of business interactions,
- discontinuation of services,
- closure of user accounts,
- expiration or modification of these Terms.

SECTION 15 — BUSINESS CONTINUITY & FORCE MAJEURE

15.1 Force Majeure Events

The Company shall not be held liable, responsible, or deemed to be in breach of these Terms for any failure, delay, interruption, suspension, or deficiency in performing any obligation, delivering any communication, or maintaining availability of its systems, where such failure or delay results, directly or indirectly, from a **Force Majeure Event**.

A Force Majeure Event includes any event or circumstance that is beyond the reasonable control of the Company, whether foreseeable or unforeseeable, including but not limited to:

- **Natural disasters**, such as floods, storms, earthquakes, lightning, fire, or other acts of God
- **Internet outages**, including disruptions to global or regional internet backbones, DNS failures, routing errors, ISP-level outages, or submarine cable failures
- **Cyberattacks**, including denial-of-service attacks, malware outbreaks, ransomware, security breaches, hacking attempts, or any malicious digital activity targeting systems of the Company or its providers
- **Government restrictions**, including directives, regulations, emergency orders, sanctions, changes in law, policy enforcement actions, or any governmental intervention affecting the Company's ability to operate
- **Infrastructure failures**, including power outages, hardware malfunctions, data centre incidents, telecom provider failures, cloud provider outages, or critical third-party system failures
- Fires, explosions, chemical events, or industrial incidents
- Strikes, labour disputes, workforce shortages, or lockouts affecting the Company or key suppliers
- Pandemic, epidemic, quarantine restrictions, public health emergencies, or disease outbreaks
- Unavailability or degradation of third-party hosting, cloud, storage, email, conferencing, or communication platforms
- Civil disturbances, riots, terrorism, war, armed conflict, or military action
- Any other event or circumstance which materially affects the Company's ability to fulfil its obligations and which could not have been reasonably prevented or mitigated.

15.2 Suspension of Obligations

During the continuation of a Force Majeure Event, the Company may:

- suspend communications,
- limit access,
- restrict system usage,
- defer obligations,
- delay responses, or
- temporarily disable functionalities

without any liability for such actions.

Any suspension will continue only for the duration of the Force Majeure Event and until operational stability can be safely restored.

15.3 No Liability for Resulting Losses

The Company shall not be liable for any:

- delay,
- inability to respond,
- transmission failure,
- missed communication,
- loss of data,
- corruption of files,
- delay in service availability,
- inability to access systems,
- degradation of performance, or
- consequential effects

arising out of or related to a Force Majeure Event.

Users understand and acknowledge that digital communication infrastructure inherently depends on numerous external providers and global systems beyond the Company's control.

15.4 Mitigation Efforts

The Company will make reasonable efforts to mitigate the impact of Force Majeure Events where feasible, including:

- implementing failover measures,
- utilising redundancy systems,
- escalating issues to service providers,
- restoring services when safe and practical.

However, such efforts shall not be construed as an admission of liability or a guarantee of continuity.

15.5 Resumption of Operations

Upon cessation of the Force Majeure Event, the Company will resume its obligations as soon as reasonably practicable.

Any resumed performance shall not be accelerated, and delays caused by the event shall be deemed excusable.

15.6 Extended Force Majeure

If a Force Majeure Event continues for an extended period of time, the Company may, at its discretion:

- modify operational processes,
- reduce or alter services,
- prioritise critical communications,
- permanently discontinue certain channels or features.

Such actions will not create liability or entitle Users to claims.

SECTION 16 — LIMITATION OF LIABILITY

16.1 Maximum Liability

To the maximum extent permitted under applicable law in both the United Kingdom and India, the total aggregate liability of the Company — including its subsidiaries, affiliates, directors, officers, employees, contractors, and agents — arising out of or relating to:

- any communication or exchange of information,
- any use or attempted use of Company systems,
- any reliance placed on information provided by the Company,
- any operational or technical interaction with the Company, or
- any matter governed by these Terms

shall be strictly limited to the lesser of:

1. **the actual amount (if any) paid by the User to the Company specifically for the communication giving rise to the claim**, or
2. **the minimum liability amount required by applicable law**, if such law mandates a non-excludable financial obligation.

Users acknowledge and agree that communications, support interactions, and information exchanges are not services for which separate fees are typically charged, and therefore the Company’s liability is inherently limited.

This limitation applies regardless of the form of action, including but not limited to contract, tort (including negligence), statutory breaches, or any other legal theory.

16.2 No Consequential, Indirect, or Special Damages

Under no circumstances shall the Company be liable for any form of:

- indirect loss,
- consequential loss,
- incidental damages,
- exemplary or punitive damages,
- loss of profits,

- loss of business,
- loss of opportunity,
- loss of anticipated savings,
- loss of use,
- loss of reputation or goodwill,
- loss or corruption of data,
- business interruption, or
- any other category of damages that are not direct and strictly quantifiable.

This exclusion applies **even if**:

- the Company has been advised of the possibility of such damages,
- such damages were foreseeable, or
- such damages arise from the failure of any safeguard, warning, or disclaimer.

16.3 Disclaimer of Warranties

All communications, whether written, verbal, digital, automated, or otherwise transmitted by the Company, are provided strictly on an **"as is", "as available", and "as provided" basis**.

To the fullest extent permitted by applicable law, the Company expressly disclaims all representations, guarantees, and warranties, whether:

- express or implied,
- statutory or contractual,
- arising from course of dealing or usage of trade, or
- assumed by virtue of communication or interaction.

This includes, without limitation, any implied warranties of:

- accuracy,
- completeness,
- reliability,
- merchantability,
- fitness for a particular purpose,
- non-infringement,
- error-free transmission,
- timeliness or promptness of response,
- secure, uninterrupted, or virus-free communication, or
- suitability of communicated information for commercial or legal reliance.

Users acknowledge that:

- communications may contain errors, delays, incomplete information, or operational constraints;
- communications should not be solely relied upon for critical decisions;
- professional, legal, technical, or financial advice must not be inferred from any communication.

16.4 Scope of Limitations

These limitations apply:

- regardless of the jurisdiction in which a claim is brought,
- regardless of whether liability is alleged contractually or tortiously,
- to all forms of communication channels described in these Terms,
- to all legal theories, regardless of whether known or unknown at the time of the communication.

16.5 Mandatory Rights Not Affected

Nothing in this section shall exclude liability where exclusion is not permitted under applicable law.

Where certain rights cannot be disclaimed, the Company limits liability **only to the minimum extent permitted**.

SECTION 17 — INDEMNITIES

17.1 General Indemnification Obligation

You agree to fully indemnify, defend, and hold harmless the Company, its subsidiaries, affiliates, directors, officers, employees, contractors, representatives, and agents from and against any and all claims, actions, proceedings, liabilities, losses, damages, penalties, fines, settlements, judgments, costs, and expenses (including reasonable legal fees and expenses) arising out of or relating to:

- your misuse, abuse, or unauthorised use of any communication channel;
- your breach or violation of these Terms;
- your infringement of any intellectual property rights, confidentiality obligations, or privacy obligations;
- your transmission of harmful, illegal, or inappropriate content;
- your circumvention or attempted circumvention of security measures;
- your participation in fraudulent, malicious, or prohibited activities;
- your failure to comply with applicable law while interacting with the Company; or

- any action, inaction, or negligence on your part that results in harm or risk to the Company.

17.2 Indemnification for Technology & System Abuse

Without limiting the foregoing, this indemnity includes losses stemming from:

- attempts to hack, breach, or bypass Company systems;
- attempts to access information without proper authorisation;
- misuse of APIs, automation tools, or system interfaces;
- introduction of malware, viruses, or harmful code;
- disruption, degradation, or interference with Company operations;
- manipulation or misuse of logs, audit trails, or system records.

17.3 Defence & Cooperation

If the Company becomes aware of any claim subject to indemnification under this section, the Company may:

- assume control of the defence at its discretion;
- require you to cooperate fully in investigations, defence strategies, or settlement discussions;
- require you to provide documents, communications, and information needed to address the claim.

Failure to cooperate may itself constitute a breach of these Terms.

17.4 Survival of Indemnity

Your indemnification obligations survive:

- termination of any communication or relationship with the Company,
- cessation of use of Company systems,
- updates or modifications to these Terms, and
- closure of any account or channel.

This ensures the Company remains protected against earlier misconduct or misuse.

SECTION 18 — NOTICES & AMENDMENTS

18.1 Updates & Amendments

The Company reserves the full and unconditional right, at its sole discretion and at any time, to update, modify, amend, supplement, replace, or revise these Terms in whole or in part. Such updates may occur:

- to reflect regulatory or legal changes,
- to incorporate new operational practices,
- to enhance security or monitoring frameworks,
- to clarify responsibilities and scope, or
- to support new technologies, features, or business needs.

Updates may be made **without prior notice**, and your continued communication or interaction with the Company constitutes acceptance of the updated Terms.

The Company is under no obligation to notify you individually of changes, and it is your responsibility to review the most current version when engaging with the Company.

18.2 Publication & Availability

The latest and most authoritative version of these Terms will always be made available at the designated Company URL or other official online location as determined by the Company.

The version published online supersedes all previous versions, drafts, communications, or understandings.

Users are deemed to have constructive notice of the updated Terms by virtue of their availability at the published URL.

SECTION 19 — GOVERNING LAW & JURISDICTION (DUAL)

19.1 United Kingdom

For all communications, transactions, interactions, exchanges of information, or matters that arise within, relate to, or are deemed to be connected with the Company's operations, activities, personnel, systems, infrastructure, or contractual relationships in the **United Kingdom**, the following shall apply:

- The interpretation, construction, validity, and enforcement of these Terms shall be governed exclusively by the laws of **England and Wales**, without giving effect to any principles of conflict of laws that would require the application of the laws of any other jurisdiction.
- Any dispute, controversy, claim, or cause of action — whether contractual, statutory, tortious, or otherwise — arising out of or connected with UK-based interactions shall fall within the **exclusive jurisdiction of the courts of England and Wales**.

- Users expressly consent to the personal and subject-matter jurisdiction of such courts and agree that these courts represent a fair and appropriate venue.

Nothing in this clause shall restrict the Company's ability to seek emergency injunctive or equitable relief in any jurisdiction where such relief is required.

19.2 India

For all communications, interactions, exchanges of information, business dealings, or matters that arise within, relate to, or are connected with the Company's presence, staff, clients, systems, operational footprint, or contractual relationships in **India**, the following shall apply:

- These Terms shall be governed and interpreted in accordance with the laws of the **Republic of India**, including but not limited to the Indian Contract Act, the Information Technology Act, and applicable rules and regulations, without reference to conflicts-of-law provisions.
- Any dispute, controversy, or claim arising out of Indian-based interactions shall fall under the **exclusive jurisdiction of the courts located in Ongole**, and Users expressly agree to submit to such jurisdiction.
- Users acknowledge that the Indian courts provide a reasonable and proper forum for resolving India-related disputes.

As with the UK clause, the Company may pursue urgent injunctive relief in other jurisdictions when necessary to prevent harm or protect rights.

19.3 Conflict Resolution (Cross-Border Interactions)

Where communications, interactions, or matters have a **cross-border, multi-jurisdictional, or hybrid nature**—involving elements, parties, systems, or operations in both the United Kingdom and India—the Company shall have the **sole discretion** to elect which governing law and jurisdiction shall apply for the purpose of dispute resolution.

This discretionary right includes, but is not limited to:

- The choice to apply UK law and UK courts
- The choice to apply Indian law and Indian courts
- The choice to enforce rights in multiple jurisdictions simultaneously, where legally permissible
- The right to initiate proceedings in any jurisdiction where harm, misuse, breach, or unlawful activity has occurred or may occur

Users acknowledge and agree that:

- Such flexibility is essential for a global organisation

- Jurisdiction may be selected based on operational, legal, regulatory, or strategic considerations
- Users shall not challenge the Company's elected jurisdiction once chosen
- Jurisdiction selection by the Company is binding for all dispute-related purposes

SECTION 20 — MISCELLANEOUS

20.1 Severability

If any provision, clause, sub-clause, or portion of these Terms is held by a court or competent authority to be invalid, unlawful, or unenforceable under applicable law, such provision shall be deemed severed from these Terms to the minimum extent required.

The invalidity or unenforceability of that specific portion shall **not** affect the validity, legality, or enforceability of the remaining provisions, which shall continue in full force and effect as if the severed portion had never formed part of these Terms.

Where possible, any such unenforceable provision shall be replaced with a valid and enforceable provision that most closely reflects the original intent of the Company.

20.2 No Waiver

Any failure, delay, omission, or forbearance by the Company to assert, enforce, or exercise any right, remedy, power, or entitlement under these Terms shall **not** constitute a waiver of such right.

A waiver shall only be effective if provided **in writing** and signed by an authorised representative of the Company.

No single or partial exercise of a right shall prevent any further or future exercise of that right or any other right.

The Company reserves all rights not expressly waived in accordance with this clause.

20.3 Assignment

The Company may assign, transfer, delegate, subcontract, or otherwise dispose of any of its rights, obligations, or interests under these Terms, in whole or in part, at any time and without requiring prior notice or consent from any User.

Users may **not** assign or transfer their rights or obligations under these Terms without obtaining the Company's prior written consent.

Any unauthorised assignment by a User shall be deemed void and of no legal effect.

20.4 Survival

The termination, expiration, or cessation of any communication or interaction with the Company — whether by completion of a conversation, closure of an account, discontinuation of services, or otherwise — shall **not** affect the continuing application and enforceability of provisions that, by their nature or intent, are meant to survive.

This includes, without limitation:

- monitoring provisions,
- data retention and audit provisions,
- intellectual property restrictions,
- confidentiality obligations,
- indemnification requirements,
- limitation of liability clauses, and
- governing law and jurisdiction clauses.

These provisions remain legally binding and enforceable beyond the end of any communication relationship.