Service Acceptable Use Policy ("AUP")

April 2025 v2.2

1. Introduction

All intellectual property rights in this document belong to Tieva Limited ("**TIEVA**") and is for internal use and client information.

The purpose of this document is to set out the acceptable use standards that apply to the managed services ("**Services**") that TIEVA provides to you, as TIEVA's Client ("**Client**") under the Master Services Agreement, which can be accessed here ("**Master Services Agreement**"), as may be varied by the Parties.

2. Interpretation

Except as defined in this document, capitalised terms shall have the meanings given to them in the Master Services Agreement.

In the event of conflict with the terms of this document and an Order Form, the provisions of the Order Form shall take precedence over this document. In the event of conflict with the terms of this document and the Master Services Agreement, the terms of this document shall take precedence.

3. Policy

The Client is responsible for any violations of this AUP by anyone using the Services, whether authorised or not.

Any queries regarding this AUP must be addressed to the TIEVA Chief Operating Officer. TIEVA reserves the right to or suspend the Service(s) immediately should breach of this AUP occur.

TIEVA reserves the right to revise this AUP from time to time. Any change will be posted online as the latest version, we shall try to give you reasonable notice of any major changes. The Client's continued use of the Services shall constitute acceptance of any such revisions.

3.1 Internet Abuse

The internet provision within the Services must NOT be used for:

- Attempted or actual unauthorised access to data, services, systems or networks, including probe, scan, test, or breach security or authentication measures without the express permission of the owner of the system or network ("hacking");
- Attempted or actual interference with Services to any host or network including, without limitation, "mailbombing", "flooding", deliberate attempts to overload a system and broadcast attacks;
- Attempted or actual use of an internet account or computer without the owner's permission;
- Attempted or actual collecting of information by deceit, including, but not limited to "internet scamming", "password robbery", "phishing" and "port scanning";
- The creation of any false, misleading, or deceptive TCP-IP packet header or any part of the header information in an internet posting;

- Distributing software that covertly gathers information about a user or covertly transmits information about the user;
- Any activity that is likely to result in retaliation against the Services;
- Any activity related to downloading, infringing, misappropriating or transmitting copyrighted materials or another person or entities intellectual property rights including text, music, software, art, images, or other material for which the Client has no licence or does not have the express permission of the copyright owner;
- Any activity or conduct that is likely to be in breach of any applicable laws, codes, or regulations, including data protection;
- Introducing intentionally or knowingly into the Services any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Services;
- Engaging in activities, whether lawful or unlawful, that TIEVA determines to be harmful to TIEVA's operations, reputation, goodwill, or customer relations; and
- Any activity or conduct that unreasonably interferes with the use of the Services or services being provided by TIEVA to its other customers.

3.2 Email Abuse

The email provision within the Services must not be used for:

- Unsolicited bulk email contravening the Privacy and Electronic Communications (EC Directive) Regulations 2003, which states that the use of email for direct marketing is only allowed to recipients who have given their prior consent other than for market research purposes;
- Sending or relaying of unsolicited email ("spam");
- Continued issue of unsolicited email to any person who has indicated that they do not wish to receive it ("opt-out");
- Obscuring the source of email in any manner. Email must include the senders or recipients e-mail address in the body of the message or in the 'TO' line of the email;
- Use of any false, misleading, or deceptive header or part of the header information, including masking the originator, in an email; and
- Use of third party email services that do not have similar procedures covering the above points.

3.3 Offensive Content

The Service must not be used to publish, display, or transmit any materials or content that TIEVA reasonably believes:

- Constitutes or contains imagery, text, or links related to child pornography or "grooming" (this will be immediately notified to the police);
- Constitutes or contains imagery, text, or links related to pornography or is otherwise obscene or sexually explicit including manufactured images or "deepfakes";
- Constitutes or contains imagery, text or links related to violence, incitement to violence, threats, or can be construed as harassment;
- Includes reference to any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive, or menacing;
- Is defamatory or violates a person's privacy;
- Is discriminatory of age, race, religion, sex, or sexual orientation;
- Is deceptive under consumer protection laws, including chain letters and pyramid schemes;
- Creates a risk to a person's safety or health or a risk to public safety or health;

- Compromises national security or interferes with an investigation by law enforcement bodies;
- Infringes another person's trade or service mark, patent, technical copyright, or other property right;
- Involves theft, fraud, drug-trafficking, money laundering or terrorism or is otherwise illegal or solicits illegal conduct;
- Is otherwise malicious, fraudulent, or may result in offence or legal action.

3.4 Security

The Client must maintain appropriate policies and procedures for its personnel (including employees, contractors and workers) who use the Services, that requires them to adhere to the same standards as this AUP and impose appropriate disciplinary consequences on them in the event of a breach of this AUP. The Client is responsible for communicating to its personnel that communications and systems connected to Services are subject to automated monitoring.

The Client must observe and take reasonable security measures in its use of the Services, including:

- All Service user accounts should be individual and non-generic;
- Service usernames and passwords must not be shared or disclosed;
- Passwords should be reasonably complex (8-character minimum containing alpha and numeric characters with case variations);
- Passwords should be changed on a regular/cyclical basis;
- Physical access to network Service equipment (routers, switches, etc) must be secured by means of a locked cabinet and/or room;
- Copies of all Software licenses, discs, agreements, Hardware serial numbers, and local data on-site should be securely stored off-site.

3.5 Legal Compliance

TIEVA may monitor any content or traffic belonging to the Client or the Client's Service users to ensure the Service is used lawfully and in compliance with this AUP. TIEVA may intercept or block any content or traffic belonging to the Client where the Service is being used unlawfully or not in accordance with this AUP. Such interception or block will be notified to the Client by TIEVA. TIEVA is, however, under no duty to monitor or govern Client data and/or activities, and TIEVA disclaims any responsibility for any misuse of the Service by the Client or its agents or personnel.

In accordance with UK and International law, TIEVA is legally obliged to suspend the Service and/or provide data to recognised authorities such as the police and/or HM Revenue and Customs and/or the Information Commissioner's Office on demand.

3.6 IP Addressing

The Client must only use IP addresses assigned by TIEVA in its use of the Services and not take any action or inaction, which directly or indirectly results in any TIEVA IP space being listed on any abuse database.

3.7 Software and Third Party Services

The Client must not remove, copy, modify or obscure any copyright trademark or other proprietary rights notices contained in or on any software or Third Party Services provided. While TIEVA is an approved licensor of specific software and Third Party Services, all software or Third Party Services remains the intellectual property of the respective licensor.

The Client must not attempt to copy, distribute, reverse engineer, decompile, or otherwise disassemble any of the software or Third Party Services provided, except to the extent that such activity is permitted by applicable law.

'No High-Risk Use' – Software and Third Party Services is neither designed nor intended for use in a situation where such software or Third Party Services failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage. High-risk use includes but is not limited to the following examples: aircraft or other forms of mass human transportation, nuclear or chemical facilities and or medical devices.

3.8 Illegal Activities

TIEVA will, without notice to the Client, report to the appropriate authorities any action or conduct of the Client and/or its personnel that it believes is illegal.