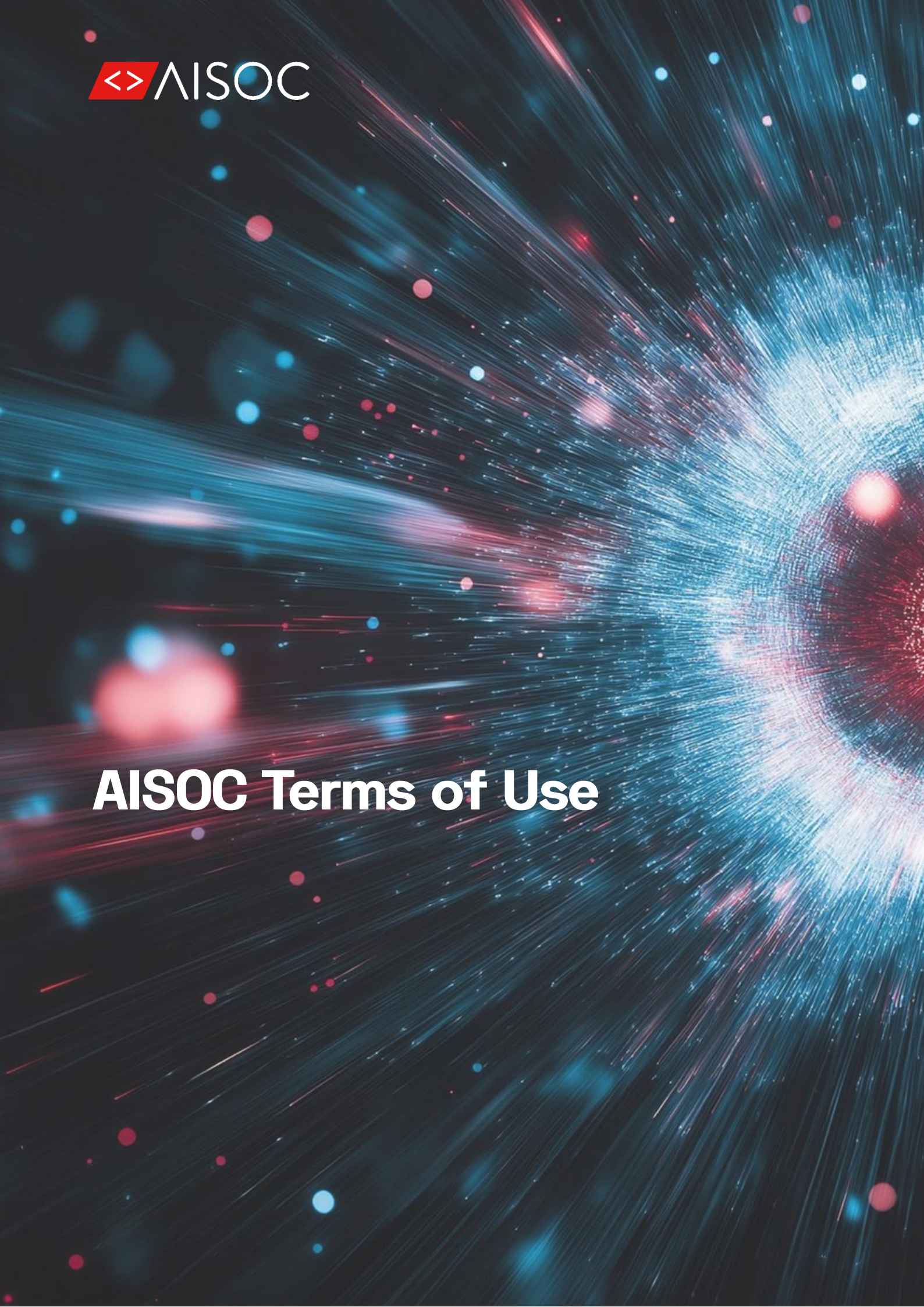

AISOC Terms of Use

Contents

1. Introduction

This document sets out the Terms of Use for AISOC, a Software-as-a-Service (SaaS) solution.

Definitions:

• **Provider:** Refers to AISOC, the entity that owns, operates, and delivers the SaaS solution described herein, including all associated infrastructure, support services, and intellectual property.

• **Customer:** Refers to the entity using the SaaS solution.

• **User:** Refers to a person who is authorized by the Customer to access or use AISOC (including its web interface and related services) under the Customer's account such as employees, contractors, and other permitted agents acting solely for the Customer's internal business purposes and in accordance with this Agreement.

• **Log:** Refers to a timestamped record of system or security-relevant activity generated by a technology component and ingested by a Security Information and Event Management (SIEM) system or other security system for analysis and correlation.

• **Incident:** Refers to a security-related event or set of correlated events, originating from a SIEM system or other security system, that indicates a potential or actual compromise of the confidentiality, integrity, or availability of information systems, applications, or data.

• **Case:** Refers to a logical aggregation of one or more related Incidents, together with associated Logs if available, contextual data, prediction, and outcome. A Case is created by AISOC to provide a consolidated view of a security situation.

2. Description of Service

The Provider offers AISOC as a SaaS solution, providing cybersecurity services including incident processing, alerting, reporting, and related support.

2.1 Incident Processing and Alerting

Incident processing includes:

1. Receiving incidents and related logs from Security Information and Event Management (SIEM) or other similar systems and related data.

2. Preprocessing incident and log data.

3. Performing predictions and contextualization.

4. Triaging and grouping incidents into cases.

Incident alerting includes:

• Notifying the Customer or relevant third parties of contextualised incidents that might require further attention based on AISOC's predictive algorithm.

• Collecting feedback from recipients of incident notifications.

2.2 Incident Reporting

Incident reporting is provided via a web interface, offering the Customer a holistic view of AISOC operations, including:

- Processed incidents, and AISOC cases
- Related logs
- Performance metrics
- Feedback

2.3 Support and Feature Requests

Support and feature requests cover queries raised by the Customer related to:

• Advice on AISOC functionalities

• Access to services

• Technical issues with incident processing, alerting, or reporting

• Standard changes or modifications to features

Note: Cybersecurity consultancy or advice is not included and may be provided separately as part of managed services or SOCaaS.

3. Service Levels and Uptime Commitments

SLAs, uptime commitments, and scheduled maintenance are described in AISOC SLA.pdf.

3.1 Request Prioritisation

Requests are prioritised based on the impact on AISOC services and the Customer's operations:

Priority Description Example

P1 – Critical

The AISOC service is unavailable, and significant users are unable to perform their daily work, resulting in a backlog. System outage is preventing incident processing.

P2 – High

Service is partially available; significant users are affected. Delays in incident notifications.

P3 – Medium

Service is available but not performing optimally, resulting in minor user impact.

Minor configuration issue.

P4 – Low

Service is fully available, no impact on daily operations—request for advice or information.

Feature Requests:

• Feature requests invoked through a Support request are subject to SLA timelines.

• Other feature requests do not have SLAs unless agreed contractually.

4. Data Protection and Security

4.1 Compliance with local law

The Provider shall comply with all applicable data protection laws from the country where data is processed.

4.2 Roles and Responsibilities

• Customer: Data Controller

• Provider: Data Processor

The Provider will process personal data only in accordance with documented instructions from the Customer, unless legally required to do otherwise.

4.3 Data Breach Notification

In the event of a personal data breach, the Provider will notify the Customer without undue delay, and where feasible, within 24 hours, including all relevant information for breach reporting in line with legal obligation.

4.4 Use of Sub-processors

• Sub-processors may be engaged under equivalent data protection obligations.

• The Provider remains liable for sub-processor actions.

• The Customer will be notified of changes to sub-processors and may object.

4.5 Privacy Policy

The Data Privacy document outlines the scope, nature, and purpose of processing Customer data, in compliance with relevant authority from country where data is processed.

5. Prohibited Uses

AISOC is intended solely for civilian cybersecurity purposes. The Customer agrees not to use AISOC for:

• Military or law enforcement operations, including surveillance, intelligence gathering, or tactical decision-making.

• Civilian applications that could be repurposed for military or law enforcement use.

6. Intellectual Property Rights

6.1 Ownership of Software

The Provider retains all rights, title, and interest in the SaaS solution, including software, source code, documentation, and updates. No ownership rights are transferred to the Customer.

6.2 License Grant

The Provider grants the Customer a non-exclusive, non-transferable, revocable license to access and use the SaaS solution solely for internal business purposes until termination of the Agreement.

6.3 Customer Data

All data provided by the Customer ("Customer Data") remains the Customer's property. The Provider will process such data only in accordance with the Customer's instructions and applicable laws.

7. Changes to the Service

7.1 Right to Modify

The Provider may update, enhance, or discontinue features, provided that overall functionality is not materially degraded.

7.2 Customer Notification

Material changes affecting the Customer's use will be communicated in advance via email or other reasonable means.

7.3 Right to Terminate

If a material change adversely impacts the Customer's use, the Customer may terminate the Agreement within 30 days of receiving notice.

8. Term and Termination

8.1 Contract Duration

This Agreement commences on the Effective Date and remains in effect until terminated in accordance with its terms.

8.2 Termination Rights

Either party may terminate:

• For convenience, with 30 days' written notice.

• Immediately, for material breach not cured within 30 days.

• If the other party becomes insolvent, enters liquidation, or ceases business.

8.3 Data Access and Transition Assistance

Upon termination:

• Customer has 30 days to access/export data.

• Provider will assist with secure data transfer (fees may apply for extended assistance).

• Customer Data will be deleted after this period unless retention is required by law or agreed otherwise.

9. Limitation of Liability

9.1 General Limitation

To the maximum extent permitted by law, the Provider is not liable for indirect, incidental, special, consequential, or punitive damages, including loss of profits, data, or business opportunities.

9.2 AISOC Output Disclaimer

The Customer is responsible for reviewing and validating outputs, predictions, or classifications generated by AISOC. The Provider does not guarantee accuracy and is not liable for reliance on inaccurate or incomplete information.

9.3 Liability Cap

The Provider's total liability is limited to 25% of fees paid by the Customer in the six months preceding the claim.

Contact

0330 390 2040

hello@aisoc.cloud

www.aisoc.cloud

@aisoccloud

aisoccloud