PRODUCT ANNEXURE – THREAT EXPOSURE MANAGEMENT

1. INTRODUCTION

This Annexure sets out the legal framework for the provision and use of the Flare Platform Services provided by the Supplier. This Product Annexure is subject to and must be read in conjunction with the Supplier terms and conditions located at https://saicom.io/ and the licensor specific documentation referred to in and located at https://docs.flare.io/. The nomenclature used in the Agreement shall apply to this Product Annexure.

2. DEFINITIONS

2.1. **Flare Platform** - means the web application, mobile application, search bar, search API, application programming interface, software and other components described in the Documentation, and made available to Customer pursuant to an Order Document, as part of the Services, for the duration of the Term.

2.2. **Identifier** - means an asset, such as a fully qualified domain name, an IP address, keyword, brand, product, person, or any other identifier type available in the Flare Platform, which is monitored by Customer using the Services.

2.3. **Intended Purpose** - means to prevent fraud, defamation, abuse of rights, crimes, and incidents, including for threat intelligence purposes, such as to monitor the dark web for leaked data.

2.4. **Monitoring Services** - means the use of the Flare Platform to monitor dark web forums, open ports, S3 buckets, ransomware blogs, public GitHub repositories, paste sites, dark. web marketplaces, dark web chats, threat actors' profiles, infected device market, illicit telegram markets and similar data sources as determined by Flare from time to time (the "Monitored Sources").

2.5. **Public Data** - means all data and content made available to you through Monitored Sources, including those retrieved through the Retrieval Function, or any other publicly available content available through the Flare Platform.

2.6. **Retrieval Function** - means a functionality of the Flare Platform that allows for the retrieval of data, software, content, or material from the Monitored Sources. A retrieval includes the extraction, download, control, and possession.

2.7. **Services** - means the services provided by the Supplier and/or the Licensor pursuant to an Order Document, including, as applicable, access and use of the Flare Platform, Identifiers, Service Credits and Documentation. The Services include the Technical Support, the Threat Intelligence Services, Monitoring Services, and the Take Down Services.

2.8. **Take Down Services** - means the Services provided by Flare to attempt to obtain the removal or take down of domains, social media profiles, and other permitted take downs, as described in the Documentation.

2.9. **Query Identifier** - means a type of Identifier that may be used to string multiple query words, and which are used as part of the Flare Platform, including for the Monitoring Services

3. SERVICES

3.1. The Services leverage artificial intelligence to provide insights and contextual analysis based on Public Data and Customer Data, including to generate Intelligence Data. Customer acknowledges and understands that the use of artificial

intelligence is not error-free and may produce unexpected or inaccurate results. Flare does not guarantee the accuracy, completeness, or reliability of the results produced using artificial intelligence technologies. The quality, reliability and completeness of the Intelligence Data depend on the quality, reliability and completeness of Public Data which are not within the Supplier or its Licensor's control. Customer is responsible for conducting reasonable verification on the Intelligence Data, or otherwise, on the content made available through the Flare Platform.

3.2. The Services may only be accessed by a Customer via an account set up for the Customer by the Supplier.

3.3. The Customer is responsible for keeping its credentials confidential and cannot share them with anyone. If the Customer suspects that its account is compromised or if it loses its credentials, Customer must immediately inform the Supplier. So that the account can be blocked, or the passwords reset, as the case may be.

3.4. Each Identifier may only be assigned once per calendar month. Customer is solely liable for determining the number and nature of the Identifiers adequate for its needs. Identifiers can only be used on corporate assets or other assets which Customer is authorized to monitor. Customer can configure the Flare Platform to generate alerts for Identifiers. Real-time alerts are provided through the Flare Platform. Customer is responsible for monitoring the Flare Platform.

3.5. Any additional Identifiers purchased by the Customer during the Term reflected in the Order Document, will only be valid for the remaining duration of the then current Term.

3.6. The Customer may exchange Service Credits for Services. The Supplier will inform the Customer of the number of Service Credits for a required for the Service request. Service Credits can be used monthly and are valid for one month, any unused Service Credits available to the Customer for a particular month will expire at the end of that month. Unused Service Credits cannot be rolled over to the following month.

3.7. The Flare Platform can be configured to generate alerts, including in the context of the Monitoring Services. The Customer is responsible for following up on these alerts, for determining the appropriate remediation actions and for taking such actions. Any advice provided to you, through the Documentation or otherwise, is only for information.

3.8. The Take Down Services are only provided for domain names and social media profiles (excluding specific posts) unless agreed otherwise in writing by the Licensor. Neither the Supplier nor the Licensor control third parties' response time to take down requests, further a request may not be successful. Even if Take Down Services are successful, other domains and social media profiles may continue to appear or may continue to exist. Supplier will keep Customer reasonably informed of the progress of any Take Down Services.

3.9. The Supplier does not warrant or guarantee that the Services (including the Flare Platform) will be compatible or interoperable with Third-Party Services.

3.10. If Customer requests Threat Intelligence Services, The Supplier will deploy reasonable efforts to provide the Threat Intelligence Services without unreasonable delays. If Customer must obtain the Threat Intelligence Services within 24 hours, each Service Credit required for the request will be required twice.

3.11. The Supplier will provide the Technical Support in accordance with this Product Annexure, including any Improvements made to the Flare Platform during the Term. The Flare Platform will be available based on the Uptime specified herein. Customer is responsible for provisioning End Users' accesses to and configuring the Flare Platform. The Supplier not responsible for End Users' failure to protect the confidentiality of their credentials. Customer will suspend access to compromised accounts.

4. ACCEPTABLE USE

4.1. Customer will only use and authorize the use of the Retrieval Function in accordance with applicable laws. Customer must have the rights to access and retrieve Public Data. Customer understands that accessing and retrieving Public Data in violation of the foregoing obligations may results in criminal sanctions. Public Data which is retrieved or accessed through the Retrieval Function may contain security issues, harmful content, and stolen properties. The Supplier and its Licensors will have no liability for Losses resulting from Customer's use of the Retrieval Function in violation of the foregoing.

4.2. Customer will access and use the Services for lawful and internal business purposes, including for threat intelligence, information security, information privacy, monitoring and protecting corporate assets. Customer will not use the Services for unlawful monitoring, in breach of individuals' privacy, or in violation of a third party's IP. Customer will only use and authorize the use of the Services, including the collection of from Monitored Sources, in accordance with applicable laws, and the terms of the.

4.3. Customer is responsible for the acts and omissions of its End Users. In case of a violation or imminent violation of this the acceptable use, the Supplier will have the right to suspend Customer's access and use of the Services to the extent necessary to cure such breach. The Supplier will provide a prior notice to Customer, unless it is prevented to do so by the circumstances of the suspension, in which case, the Supplier will notify Customer as soon as reasonably possible.

5. TERM AND TERMINATION

5.1. In the event that the Customer wishes to terminate the Services, written notice of non-renewal at least 30 days prior to the end of the then-current Term must be provided to the Supplier. Failure to provide written notice of termination as aforesaid will result in the Term automatically renewing for successive periods of 12 months at the then-current Fees for the Services.

6. DISCLAIMERS

6.1. THE RETRIEVAL FUNCTION ALLOWS USERS TO ACCESS AND REQUEST THE RETRIEVAL OF PUBLIC DATA. THE PUBLIC DATA MAY CONTAIN MALICIOUS CODES, HARMFUL CONTENT, THIRD PARTY IP, AND INDIVIDUALS' PERSONAL DATA. THE PUBLIC DATA IS NOT SCANNED FOR SECURITY ISSUES. POSSESSION OF STOLEN MATERIAL WHICH YOU ARE NOT AUTHORIZED TO ACCESS MAY LEAD TO CRIMINAL INFRACTIONS. YOU MUST HAVE THE RIGHT TO ACCESS AND OBTAIN POSSESSION OF THE PUBLIC DATA THROUGH THE RETRIEVAL FUNCTION. NEITHER FLARE NOR ITS REPRESENTATIVES WILL BE LIABLE FOR ANY LOSSES RESULTING FROM THE USE OF THE RETRIEVAL FUNCTION OR ACCESS TO PUBLIC DATA. FLARE HAS NO CONTROL WHATSOEVER ON. THE PUBLIC DATA. FLARE HAS NO RESPONSIBILITY WHATSOEVER FOR LOSSES RESULTING FOR THE USE OR ACCESS TO PUBLIC DATA.

The Customer uses the Services and the Flare platform at its own risk. A sandbox and other precautions should be considered

7. SERVICE FEES AND CHARGES

7.1. Service Fees shall be provided at the rates set out in the Order Document, plus applicable taxes. The Supplier may from time to time modify the Fees.

8. RESTRICTIONS

8.1. Customer will not use or access, nor permit the use or access of, the Services to:

8.1.1. share credentials among End Users or among End Users and third parties, to distribute, disclose or use any of the Services in any format to or by unauthorized third parties;

8.1.2. use any robot, script, spider, scraper, scraping tool, macro, bot, crawler, deep link, or other similar automated data gathering or extraction tools;

8.1.3. penetrate our security or contour our security controls; or

8.1.4. modify, reconstruct, decompile, disassemble, decipher, decrypt or otherwise reverse engineer including to discover any source code or ideas or algorithms of any portion of the Services. Using the Services for benchmarking activity or in connection with the development of any services or products that are competitive with, or derivatives of, the Services (including the Flare Platform) also is strictly prohibited.

8.2. The licensor and/or the Supplier may terminate the Customer's use of the flare Platform and Services referred to in this Annexure, together with the licences and other rights herein, immediately without notice if the Customer breaches or fails to comply with any of the terms and conditions of this Annexure or the Contract Documents or for other reasons as stated in the licensor's other documentation. The Customer agrees that, upon such termination, it will cease using the Flare Platform.

9. TECHNICAL SUPPORT

9.1. Technical Support is provided from Monday to Friday, 9 AM to 5 PM ET, excluding for statutory holidays applicable in Canada (the "Operating Hours") to End Users by way of support tickets. The Technical Support is available for the Flare Platform's current version, or otherwise, as indicated in the Documentation. Each support ticket is addressed based on its severity. Flare will respond to support tickets within the response time and will conduct commercially reasonable efforts to resolve such support ticket without undue delays.

Ticket Severity	**Response Time**
Emergency - An emergency support ticket includes a general unavailability of the Flare Platform, or the inability to use the critical functionalities of the Flare Platform.	4 hours during Operating Hours
High — A high severity support ticket includes the unavailability of critical functionalities, or material issues with accessing and using the critical functionalities of the Flare Platform.	12 hours during Operating Hours
Regular — A regular support ticket generally does not affect critical functions of the Flare Platform, or workarounds are available.	36 hours during Operating Hours

9.2. AVAILABILITY TARGET

9.2.1. The Flare Platform will be available 365 days per year, 24 hours per day, with an Uptime of 98.5%. “Uptime” means the number of minutes during which the Flare Platform is available in each month, when such availability is defined as the accessibility, usability and reasonable performance of the critical functionalities of the Flare Platform. Uptime is available in real time, and reporting data on the Uptime is available for up to 30 days, at: https://status.flare.io.

9.3. EXCLUSIONS

9.3.1. The Uptime requirements in this Product Annexure will not apply during scheduled downtime, which shall be of a maximum of 4 hours per month. The Supplier will deploy commercially reasonable efforts to inform Customer of maintenance periods, except if such notice is not practicable, such as if the maintenance period is of less than 30 minutes or for an urgent security patch.

9.3.2. The obligations set out in respect of Technical Support do not apply if caused or resulting from (a) an event of force majeure; (b) Third-Party Services; (c) the use of the Services in violation of the Flare End User License Agreement; (d) Customer’s unauthorized acts or omissions and (e) unsupported versions of the Flare Platform.

END OF ANNEXURE

On behalf of Saicom Voice Services (Pty) Ltd

Signed at _____ on the _____day of _____ 20__

_____

Signature

_____

Full Name

_____

Title

who warrants that they are duly authorised hereto

On behalf of {Client_Name}

Signed at _____ on the _____ day of _____ 20__

t +27 (0) 10 140 5000 e sales@saicom.io w saicom.io

Signature

Full Name

Title

who warrants that they are duly authorised hereto