PRODUCT ANNEXURE – MESSAGING SECURITY AND PHISHING SOLUTION

1. INTRODUCTION

This Product Annexure sets out the legal framework for the provision and use of Email Security and Phishing solution 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/. The nomenclature used in the Agreement shall apply to this Product Annexure.

2. DEFINITIONS

2.1. **"Platform"** means the messaging security platform and anti-phishing solution provided by the Supplier under the Agreement;

3. MESSAGING SECURITY PLATFORM AND PHISHING SOLUTION

3.1. **License Grant.** Subject to the terms of use of the Platform, the Customer is granted a worldwide, non-exclusive, time-limited, non-transferrable, non-sub licensable right and license, during the Term, for its authorized users to access and use the Platform solely for Customer's internal business purposes and in accordance with the Platform documentation (the **"Subscription"**).

3.2. For the avoidance of doubt: (i) the Subscription is subject to the applicable Subscription Scope, and Customer shall not use any technical or other means within, or external to, the Platform to exceed or circumvent the Subscription Scope, (ii) the Platform is only licensed or provided on a subscription basis (and is not sold). Any rights not expressly granted are reserved by the licensor, and, except for the Subscription, Customer is granted no other right or license in or to the Platform.

3.3. **Usage Restrictions**: The Customer shall not (1) sell, assign, transfer, lease, rent, distribute, resell, sublicense, lease, time-share or otherwise make the Platform available to a third-party (such as offering it as part of a time-sharing, outsourcing or service bureau environment); (2) attempt to gain unauthorized access to the Platform or disrupt the performance of the Platform; (3) modify, adapt, translate, copy, create public Internet "links" to, "frame", or "mirror" or make derivative works based on the Platform (including any data provided and/or included therein which is not Customer Data); (4) decompile, disassemble, decrypt, extract, reverse engineer or otherwise attempt to derive the source code, underlying algorithms or non-literal aspects (such as the underlying structure, sequence, organization, file formats, non-public APIs or ideas) of the Platform; (5) remove, conceal or alter any copyright, trademarks or other proprietary rights notices displayed on or related to the Platform; (6) use the Platform in a manner that violates or infringes any rights of any third party, including but not limited to, privacy rights, publicity rights or intellectual property rights; (7) use or access the Platform to build a competitive product, platform or service or copying its features or user interface, as well as product benchmarking or other comparative analysis for any external use; (8) publicly perform, display or communicate the Platform; (9) circumvent, disable or otherwise interfere with security-related or technical features or protocols of the Platform; (10) store or transmit any robot, malware, Trojan horse, spyware, or similar malicious item intended (or that has the potential) to damage or disrupt the Platform, or use any robot, spider, scraper, or any other automated means to access the Platform; (11) employ any hardware, software, device, or technique to pool connections or reduce the number of users indicated in the Order; (12) forge or manipulate identifiers in order to disguise the origin of any Customer Data; (13) take any action that imposes or may impose (as determined in the licensor's reasonable discretion) an unreasonable or disproportionately large load on the servers, network, bandwidth, or other cloud infrastructure which operate or support the Platform, or otherwise systematically abuse or disrupt the integrity of such servers, network, bandwidth, or infrastructure; (14) use the

Platform in connection with any stress test, penetration test, competitive benchmarking or analysis, or vulnerability scanning, or otherwise publish or disclose (without licensor's prior express written approval) any of the results of such activities or other performance data of the Platform; or (15) use the Platform to circumvent the security of another person's network/information, develop malware, or for any unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction.

3.4. **Fraudulent Use of the Platform**. The Customer's use of the Platform may be suspended if the Customer's use of the Platform (or any authorized user on its behalf) is deemed to be fraudulent or outside the scope of the license granted herein, by the Supplier and/or its licensor.

4. INCIDENT MANAGEMENT AS A SERVICES

4.1. The Ironscales Incident Management as a Service ("IMaaS") is a 24/7/365 worldwide managed service for users of the Platform. The Platform identifies suspicious emails and auto-classifies them. Additional work is then performed by the Customers to further classify such e-mails into different categories (e.g., malicious, spam, unknown, valid etc.).

4.2. The IMaaS acts as a supplement to the efforts of the Customer's security teams by providing a team of Supplier threat response experts to be available to facilitate investigation, analysis, and resolution of threat incidents reported by Customer's Office 365 mailbox users, as well as investigation of suspicious low-confidence incidents that may be detected by the underlying Customer Information System (CIS) system.

4.3. The IMaaS team will leverage its experience with myriad cyberattacks and evasive phishing attacks across numerous organisations and industries to help the Customer understand the methods of attacks that pose a threat to its enterprise, while making sure that reported incidents are taken care of expeditiously. Such supplemental assistance serves to lessen the burden of Customer's Security Operations Control (SOC) and IT staff by providing tactical awareness of its Office 365 security. Threats will be investigated, identified, and validated (or not). For actual, validated threats, the IMaaS team will initiate remediation efforts to thwart such phishing attacks or to otherwise classify certain correspondence as nuisance emails.

5. REQUIREMENTS AND ASSUMPTIONS

5.1. Customer must ensure it is available for discovery sessions on MS Teams or Zoom to become familiar with IMaaS and the team.

5.2. The Supplier may recommend third-party vendor products and services, as well as communicate with such vendors on the Customer's behalf, but the Supplier does not guarantee and shall not be responsible or liable for such products and services.

5.3. Given the nature of the IMaaS service and the complexity of phishing attacks, cyber security incidents, the Supplier and its Licensor do not guarantee the identification or resolution of attacks or cyber security incidents.

6. TERMINATION

6.1. The subscription term under an Order (referred to therein as the "Subscription Period") shall be as set forth in such Order, and if no such term is set forth, the subscription shall continue on a month-to-month basis from the effective date of such Order. Either party may terminate the subscription at any time by providing the other party with not less than forty-five (45)

days' prior written notice of termination (the "Cancellation Notice Period"). Such termination shall be effective upon the expiration of the applicable forty-five (45) day notice period.

6.2. The Fees payable for the Subscription shall escalate annually by an amount directed by the Licensor. The Supplier shall pass on any such annual escalation to the Customer in accordance with the Licensor's terms of use.

6.3. The Services under this Product Annexure used by the Customer may not be cancelled during the Subscription Period and must be terminated in accordance with clause 6.1 prior to the end of the Subscription Period to avoid automatic renewals of the Subscription Period.

END OF ANNEXURE