SERVICE ANNEXURE - PENETRATION TESTING SERVICES

1. INTRODUCTION

This Annexure sets out the legal framework for the provision and use of penetration testing Services provided by the Supplier. This 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 Annexure.

2. PENETRATION TESTING SERVICES

2.1. The Supplier offers the following types of penetration testing:

2.1.1. **Blackbox Testing:** Mimics an external attacker with no prior knowledge of the system, focusing on identifying and exploitation of vulnerabilities from outside the network and attempting to move laterally deeper into the network, which help businesses determine and prioritise their current risks and improve their overall security posture.

2.1.2. **Greybox Testing:** Provides the testing team with limited information about the internal structure of the target network, system, or application, offering a comprehensive security assessment.

2.1.3. **Whitebox Testing:** Offers complete transparency on the network, system or application being tested, allowing for highly detailed and targeted assessments.

2.1.4. **Web Application Penetration Test:** A thorough examination of web applications or platforms to identify security vulnerabilities, including API testing, following established methodologies like OWASP Top 10 and PTES.

2.1.5. **Social Engineering Test:** Evaluates the human element of cybersecurity by testing organisation members' susceptibility to social engineering tactics, such as phishing.

2.1.6. **Open-Source Intelligence (OSINT):** Utilises public sources, social media, and the Dark Web to gather information that could be utilised by attackers to formulate targeted attacks, highlighting potential areas for improvement in security awareness and posture.

2.2. It is recommended that penetration testing be conducted once annually. However, high-risk industries might require testing more often. Penetration testing should also be conducted after major changes to network, system or application architecture, functionalities, or features.

2.3. The duration of a penetration test is dependent on the complexity of the environment or web application and the objectives that are to be achieved. The duration of a test with a small scope can be 2 - 3 days, with a large scope test lasting 2 weeks or more.

2.4. A penetration testing report typically includes an executive summary, detailed findings categorised by severity, evidence of exploitation (if applicable),

recommendations for remediation, and technical details such as screenshots, logs, and exploit code. The report should be clear, concise, and actionable, enabling organisations to prioritise and address identified vulnerabilities effectively.

3. SUPPLIER OBLIGATIONS

3.1. The Supplier will provide the Services specified in the Proposal. Any other cybersecurity assessment, audit or additional consulting services will be subject to a separate Proposal.

3.2. The Supplier will update the Customer when each testing period starts and finishes and will immediately notify the Customer upon discovery of a critical issue which could allow an adversary access to a system, the network, or sensitive data, providing remediation actions to mitigate the risk.

3.3. The Supplier does not warrant that every vulnerability in the Customer's systems will be identified during a penetration test.

3.4. The Service is provided on an "as is" basis.

4. CUSTOMER OBLIGATIONS

4.1. The Customer is responsible for selecting the type of Penetration Testing Service or Services that will satisfy its needs.

4.2. The Customer shall provide the Supplier with specific IP (Internet Protocol) addresses and domains as may be required by the Supplier in order to perform the testing type selected by the Customer.

4.3. The Customer shall select a contact person, which contact person must be available at all times during the penetration testing engagement to restore, as soon as possible, any service or system that becomes unavailable, or remediate any critical issue that requires immediate attention.

4.4. In the event that any or all of the requested Services require the Supplier to be present on-site at the Customer's location, the Customer agrees that it will provide the Supplier's Penetration Testers (PT) all necessary access to the Customer's site and network in order to provide the Services.

4.5. The Customer will specify in the Rules of Engagement (ROE) agreed upon before the commencement of the Services, any applicable restrictions for PT presence on the Customer's site or restrictions applicable to specific systems, applications, or sensitive areas, provided that such restrictions do not unreasonably inhibit the Supplier's ability to provide the Services.

4.6. The Customer acknowledges that as part of the Services it will require the PT to view machine configuration data. The Supplier agrees that its PT will avoid intentional view or transfer of any customer and user data. The Customer further acknowledges that if sniffers are used as part of the Services, it is possible that customer and/or user data will be captured.

4.7. The Supplier agrees that should any personal data be captured, the Supplier will utilise the minimum of information required for the illustration of the vulnerability

and its effect on the Customer in the final report and will destroy any sensitive data captured at the conclusion of the Service engagement.

4.8. The Customer acknowledges that there is an element of risk associated with penetration testing activities, especially to the systems tested in a production environment. This risk includes the potential for some services on the Customer's systems to be rendered unavailable during the testing process. Although this risk is mitigated by the use of experienced penetration testers, responsible testing methods and the use of tools obtained from trusted sources, it can never be fully eliminated.

END OF ANNEXURE