CYBER SECURITY – SERVICE DESCRIPTION

Penetration Testing Services

This document (“**Penetration Testing Service Description**”) contains the terms governing the provision of Penetration Testing Services by Interactive Pty Ltd (ABN: 17 088 952 023) of 461 Williamstown Road, Port Melbourne Vic 3207 (“**Interactive**”) to the Customer named in the CMS SOW that applies to this Penetration Testing Service Description (“**Customer**”).

This Penetration Testing Service Description forms part of the Agreement, also containing the Cyber Security Service Terms and (found at https://www.interactive.com.au/terms-and-conditions) and the Master Services Agreement.

1 Penetration Testing Services

1.1 Interactive will perform the Penetration Test in accordance with the CMS SOW and the Penetration Test Scoping Form.

1.2 The Customer warrants:

(a) it has given Interactive full information about the In-Scope Items, and other parts of the IT Environment as requested, to enable Interactive to perform the Penetration Test; and

(b) that all details in the CMS SOW are and remain correct.

1.3 On request from the Customer, Interactive can provide a penetration testing workflow document, which outlines the process, tools and workflow Interactive will use to conduct the Penetration Test.

1.4 Interactive will have performed the Penetration Test when Interactive determines (in its discretion, exercised reasonably) that the In-Scope Items have been suitably evaluated.

1.5 Interactive will obtain evidence of a successful Penetration Test (if any evidence is available) and, subject to the Sensitive Information clause in the Cyber Security Service Terms, provide the evidence to the Customer.

2 Customer Responsibilities

2.1 The Customer must whitelist the Interactive Penetration Testing IP address (which is set out in the CMS SOW) on the parts of the IT Environment that are designed to detect and prevent Cyber Security Threats occurring to the In-Scope Items (for example, an intrusion protection system). This IP address will be the source of all traffic for external Penetration Tests.

2.2 The Customer must ensure the In-Scope Items and information related to the In-Scope Items (such as websites, systems, IP addresses and IP address ranges) identified in the CMS SOW do not change state, condition or configuration during the Individual Term.

2.3 The Customer must not perform any deliberate manual or non-automated actions designed to influence the success or failure of the Penetration Test.

3 Reporting

3.1 Interactive will write a report detailing the findings of the Penetration Test and provide it to the Customer after completing the Penetration Test (that report is the “Penetration Test Report”). The Penetration Test Report will include:

(a) Executive summary.

(b) Issues discovered during the Penetration Test, with a summary, technical detail and risk rating for each issue.

(c) Supporting documentation which covers any known vulnerabilities (being existing common vulnerability and exposures (CVEs) discovered during testing) and relevant additional notes from Interactive’s testing team, if any.

(d) Recommendations for remediation activities to address the issues discovered during the Penetration Test.

(e) Conclusion and appendix.

(f) Web application Penetration Tests will have a OWASP WSTG table with all relevant findings.

4 Remediation and Re-Checking

4.1 Within 90 days after the Penetration Test Report is provided to the Customer and after the Customer has attempted to remediate any issues discovered during the Penetration Test, the Customer may request Interactive to retest the In-Scope Items for which issues were discovered during the Penetration Test.

4.2 Interactive is not required to remediate any issues that are identified during the Penetration Testing. The Customer may request Interactive to remediate any issues, in which case any such remediation will be performed on a best-efforts basis and will be deemed Out of Scope Work, or be subject to a separate agreement between the parties.

4.3 If Interactive rechecks any In-Scope Items for which issues were discovered during the Penetration Test after remediation, Interactive will provide a report to the Customer after completing the recheck, with:

(a) findings based on a reproduction of the same technical steps as outlined in the Penetration Test Report; and

(b) a summary of whether any remediation has been successful.

5 Payment

5.1 Interactive will invoice Service Fees as follows,

(a) 50% of the Service Fee will be invoiced on the Service Start Date.

(b) 50% of the Service Fee will be invoiced when Interactive has provided the Penetration Test Report.

6 Definitions

Approach Type means either Black Box Testing, Grey Box Testing or White Box Testing, as identified in the CMS SOW.

Black Box Testing is a form of Penetration Test where the Customer provides no prior information, and Interactive has no prior knowledge, except for the In-Scope Items and scope. The In-Scope Items are selected, and testing is conducted on a relatively blind basis without any technical data on the inner workings of the IT Environment. Depending on the system function and scenario, user accounts may be requested to simulate a more accurate Attack vector. Typically, this is closest to a real-world scenario.

Cyber Security Threat means an actual or suspected Attack in the Customers IT Environment.

Grey Box Testing is a form of testing where the Customer provides limited information or access to enhance the Penetration Test, such as services and versions running on the In-Scope Items, internal IPs and basic workflow functions. The Customer provides user accounts with various privilege levels. Penetration Testing is conducted in a slightly more focused approach with the provided information. Grey Box Testing can provide some shortcuts to achieving quality outcomes, but is less like a real-world scenario.

In-Scope Items means the IP addresses, subnets, domain names and/or subdomains identified in the CMS SOW as being in-scope for the Penetration Test.

Penetration Test means, by using the Approach Type, attempting to enter the In-Scope Items in accordance with item 1.

Penetration Test Scoping Form means the form of that name attached as an appendix to the CMS SOW.

Penetration Testing Services means the services described in this Statement of Work, including the Penetration Test and provision of report(s).

White Box Testing is a form of Penetration Test where the Customer gives full access and complete documentation information about the In-Scope Items, with access to the servers, configuration, databases and source code. This type of test is typically performed a full security audit on systems and does not represent a true adversarial Attack.