CYBER SECURITY – SERVICE DESCRIPTION

Risk Assessment Services

This document ("**Risk Assessment Service Description**") contains the terms governing the provision of Risk Assessment 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 Risk Assessment Service Description ("**Customer**").

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

1 Services Description

1.1 Interactive will provide tailored Risk Assessment Services to assist the Customer identify and manage its risks and assess the NIST-CSF level of maturity (https://www.nist.gov/cyberframework).

1.2 The Service Fee for Risk Assessment Services includes the Pre-Engagement, on-site Engagement and Risk Assessment Report. The Service Fee includes one physical location only. The Customer may request additional locations be added as Out of Scope Work.

2 Scope

2.1 The Risk Assessment Services consists of the following, each as further described in this Risk Assessment Service Description:

(a) Pre-Engagement;

(b) Engagement; and

(c) Reporting.

3 Pre-Engagement

3.1 Interactive will send the Customer two documents via email on or after the Service Start Date, these are:

(a) Customer Environment Discovery Technical: to help Interactive gain a better understanding of the IT Environment.

(b) Customer Environment Discovery Contextual: to help Interactive understand the Customer's business as a whole and help Interactive to align the risks to size, industry sector, perceived risks and historical incidents,

(those documents are the "Customer Environment Discovery Pack").

3.2 The Customer must complete and return the Customer Environment Discovery Pack to Interactive no later than 1 Business Day prior to the Pre-Engagement Meeting commencing. If the Customer has not completed and returned the Customer

Environment Discovery Pack by that time, Interactive may schedule additional Pre-Engagement Meetings such that the Customer is able to complete the Customer Environment Discovery Pack, which will each be deemed Out of Scope Work.

3.3 Interactive will facilitate a meeting ("Pre-Engagement Meeting") either at Interactive's premises, at the Customer Location or via conference call to review the completed Customer Environment Discovery Pack with the Customer and clarify any details. The Pre-Engagement Meeting will be at least 10 Business Days after the Service Start Date.

3.4 Based on the details in the completed Customer Environment Discovery Pack and the outcome of the Pre-Engagement Meeting, Interactive will:

(a) analyse the information to prepare for the Engagement; and

(b) prepare an Engagement Schedule and send it to the Customer, which will include the commencement date, time, estimated duration and location(s) of the Engagement.

4 Engagement

4.1 Interactive will conduct the Engagement by:

(a) reviewing the Customer's policies, procedures, processes, systems, environment, data and other documentation;

(b) interviewing the Customer's personnel to verify adherence to the Customer's policies and procedures; and

(c) facilitating a workshop to:

(i) assess the level of maturity against NIST-CSF (https://www.nist.gov/cyberframework); and

(ii) prepare a Cyber Risk Register by identifying, assessing and rating the Customer's cyber risks and current controls.

5 Reporting

5.1 Interactive will prepare a Risk Assessment Report, which will consist of the following:

(a) an executive summary;

(b) an overview of the IT Environment;

(c) a summary of the highest rated risks, current controls and recommended remediation plans;

(d) the results of the NIST-CSF maturity assessment;

(e) detailed analysis and recommendations;

(f) a list of artefacts sampled during the Engagement; and

(g) the approach taken to assess the level of maturity against NIST-CSF and develop the Cyber Risk Register.

5.2 Interactive will provide the draft Risk Assessment Report to the Customer within 5 Business Days after completion of the Engagement(s). If the draft Risk Assessment Report is not completed within 5 Business Days after completion of the Engagement(s), Interactive will advise the Customer of the reasons for the delay and provide the draft Risk Assessment Report when available.

5.3 The Customer must respond to and provide feedback to the draft Risk Assessment Report within 5 Business Days after receiving it. If the Customer does not provide any feedback during this time, the draft Risk Assessment Report will be deemed accepted.

5.4 Interactive will provide the final Risk Assessment Report to the Customer within 5 Business Days after activities in item 5.3 have been completed. If the final Risk Assessment Report is not completed within this time, Interactive will advise the Customer of the reasons for the delay and provide the final Risk Assessment Report when available.

5.5 Based on the details in the final Risk Assessment Report, Interactive will assist the Customer to update the Cyber Risk Register.

6 Customer Obligations

6.1 The Customer will provide Interactive with:

(a) safe access to the Customer Location as required to perform the Risk Assessment Services;

(b) access to relevant documentation, IT systems and data, including information security, IT risk, process and procedures;

(c) availability of subject matter experts and business stakeholders for documentation reviews, interviews and workshops;

(d) any information that Interactive reasonably requests to enable it to provide the Risk Assessment Services, for example, documents, process walkthroughs or other evidence of a control being in place; and

(e) OHS & Security training for the Customer Location as required, at the Customer's cost.

6.2 The Customer is responsible for the following:

(a) determining the level of risk in terms of confidentiality, integrity and availability when participating in the Pre-Engagement and Engagement activities;

(b) ensuring appropriate stakeholders attend the Pre-Engagement Meeting and/or Engagement activities, or provide sufficient contribution via email or delegated attendees;

(c) owning and managing its risks;

(d) on-going review and update of the Cyber Risk Register to ensure its currency; and

(e) implementing any remediation plans or requesting Interactive do so as Out of Scope Work.

7 Interactive Obligations

7.1 Interactive will assist the Customer to identify their cyber risks and recommend remediation plans.

7.2 Interactive will comply with the Customer's reasonable physical security and access policies while attending the Customer Location; and

7.3 Interactive will meet with the Customer as required to discuss progress, issues and results stemming from the Services provided.

8 Definitions

8.1 The following definitions apply to this Risk Assessment Service Description:

Customer Environment Discovery Pack means the documents described in item 3.1.

Cyber Risk Register means the document that lists the Customer's key cyber risks, risk rating (as a function of consequence and likelihood), current controls, recommended remediation plans and residual risk rating (as a function of consequence and likelihood after the remediation plan has been implemented).

Engagement means the services described in item 4.

Engagement Schedule means the document that outlines the date and times of the Engagement activities.

Pre-Engagement means the phase described in item 3.

Reporting means the process described in item 5.

Risk Assessment Report means the document as described in item 5.1.

Risk Assessment Services means services described in this Risk Assessment Service Description.