CYBER SECURITY – SERVICE DESCRIPTION

Security Manager Services

This document ("Security Manager Service Description") contains the terms governing the provision of the Security Manager Services provided 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 Security Manger Service Description ("Customer").

This Security Manager 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 Service Description

1.1 Interactive will provide Services. These services are the Security Manager Services.

2 Scope

2.1 The Security Manager Services assist the Customer to satisfy the Customer's risk and compliance requirements and consist of the following, each as further described in this Service Description:

(a) Cyber Security Planning; and

(b) Service Type engagement.

2.2 Interactive will meet with the Customer as required to discuss progress and results.

3 Cyber Security Planning

3.1 After the Commencement Date set out in the CMS SOW, Interactive will facilitate a meeting ("Cyber Security Planning Meeting") either at Interactive's premises, at the Customer Location or via conference call to identify and agree on the type of Security Manager Services that the Customer requires Interactive to perform during the Individual Term based on the service descriptions and obligations set out in the CMS SOW (each type of Security Manager Services set out in the CMS SOW is a "Service Type").

3.2 During the Cyber Security Planning Meeting, the Customer will disclose information to Interactive about the Customer's information security legislative, regulatory and compliance requirements, key cyber risks and previous cyber audit results.

3.3 Based on the outcome of the Cyber Security Planning Meeting, Interactive will prepare a Cyber Security Plan, which will be in the form of the template set out in Schedule 2. Once both parties sign the Cyber Security Plan, it is incorporated into, and forms part of, the Agreement.

4 Service Type Engagement

4.1 The Service Types are as follows, each as further described in Schedule 1:

(a) Cyber Internal Audit.

(b) External Audit Assisance.

(c) Supply Chain Cyber Risk Assessment.

(d) IT System Cyber Assessment.

(e) ISMS Maintenance.

4.2 Interactive will perform each Service Type set out in the Cyber Security Plan as a separate Engagement in accordance with Schedule 1 and the Cyber Security Plan.

4.3 The Customer must provide at least 10 Business Days' notice to request an Engagement, unless otherwise determined in the Cyber Security Plan. Interactive will endeavour to meet the Customer's requested timing for each Engagement on a best effort basis, unless otherwise determined in the Cyber Security Plan. Interactive's failure to meet any requested timing is not a breach of this Agreement.

5 Customer Obligations

5.1 The Customer will provide Interactive with:

(a) safe access to the Customer Location as required to perform the Security Manager Services;

(b) access to relevant documentation including but not limited to, previous audit results, customer feedback, cyber security incidents, risk assessments, IT Environment 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 Security Manager Services, for example, documents, process walkthroughs or other evidence of a control being in place; and

(e) Occupational health and safety ("OHS") & Security training for the Customer Location as required, at the Customer's cost.

5.2 The Customer is responsible for the following:

(a) ensuring appropriate stakeholders are available to contribute to the Security Manager Services activities, or provide sufficient contribution via email or delegated attendees;

(b) owning and managing its risks;

(c) approving and implementing any recommended changes to documents; and

(d) implementing any remediation plans, unless Interactive implements any remediation plans upon the Customer's request, which will be deemed an Additional Service and will be charged in accordance with item 6.2(c).

6 Payment

6.1 If the CMS SOW renews for a Further Term, Interactive will perform the Cyber Security Planning to plan for the Security Manager Services to be performed during the Further Term. The Customer will pay the Implementation Fee each time the CMS SOW renews.

6.2 Payment Terms:

(a) Notwithstanding the Master Services Agreement, Interactive shall issue invoices for the total Implementation Fee at the Commencement Date and the commencement of any Further Term.

(b) Interactive will issue invoices for the Service Fees set out in the Cyber Security Plan monthly in advance. The Service Fee is a daily fee and payable for each Service Day Interactive provides services, based on 8 Business Hours per day. The Customers liability to pay the monthly Service Fees commences from the Service Start Date.

(c) If the Customer requests that Interactive provide additional Service Days in excess of the number of Service Days agreed in the Cyber Security Plan, the Customer shall pay Interactive at the agreed daily rate set out in the Statement of Work for each additional day that Services are performed.

7 Definitions and Interpretation

7.1 In this Service Description document the following definitions apply:

Cyber Security Plan means a document, in the format of Schedule 2, which outlines the approximate dates of the Engagement activities, the type of Security Manager Services to be performed during the Individual Term, a high level description of the scope, the amount of Service Days and the Service Fees.

Cyber Security Planning means the activities described in item 3.

Engagement means the performance of each of the chosen Service Types agreed in the Cyber Security Plan.

IT System means an application used by the Customer.

Security Manager Services means the combination of the Cyber Security Planning activities and each of the selected Service Types set out in the Cyber Security Plan and described in Schedule 1. The Security Manager Services are more particularly detailed in the Cyber Security Plan.

Service Days means the number of days in a Individual Term that Interactive will perform the Security Manager Services.

Service Type means the individual description of each of the available Security Manager Services described in Schedule 1.

Schedule 1 Security Manager Services

The Security Manager Services will include some or all of the following Service Types as described in this Schedule 1. Each Service Type is a Security Manager Service in its own right and where more than one Service Type has been described in the Cyber Security Plan, they are collectively known as the Security Manager Services. The Customer may only request Engagements for Service Types specified in the Cyber Security Plan.

1 Cyber Internal Audit

This Service Type applies to Engagements for a Cyber Internal Audit.

1.1 Interactive will conduct risk-based internal audits and compliance gap assessments ("Cyber Internal Audit") as agreed in the Cyber Security Plan.

1.2 The Cyber Internal Audit consists of the following:

(a) Audit preparation:

(i) Interactive will review the Customer's key cyber risks, compliance requirements and previous cyber internal audit results; and

(ii) the parties will determine the scope of the audit.

(b) Audit engagement:

Interactive will perform one or more of the activities set out below based on thescope agreed during the audit preparation stage:

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

(ii) interview the Customer's personnel and perform process walk-throughs to verify adherence to the Customer's policies and procedures; or

(iii) review the Customer's third party policies, procedures, processes, systems, environment, data and other documentation.

(c) Reporting:

(i) Interactive will provide a draft report, which consists of:

A. internal audit objective and scope;

B. executive summary;

C. findings and recommendations; and

D. artefacts sampled during the audit.

(ii) The Customer must respond to and provide feedback to the draft report within 5 Business Days after receipt. Where feedback is provided the parties will work together to agree the content of the final report. Interactive will provide the final report as soon as reasonably practicable.

(iii) If the Customer does not provide any feedback within the 5 Business Day period, the draft report will be deemed accepted and will be deemed to be the final report.

2 External Audit Assistance

This Service Type applies to Engagements for External Audit Assistance.

2.1 Interactive will assist the Customer to prepare for an external audit by performing one or more of the activities set out below based on the scope agreed with the Customer ("External Audit Assistance"):

(a) Audit preparation assistance as agreed between the parties.

(b) Attend the auditor's interview sessions and document reviews.

(c) Facilitate a meeting to review the audit results and assist the Customer to develop remediation plans. Interactive will provide minutes to the Customer detailing the discussions had between the parties during the meeting. The Customer is responsible for the preparation of its own remediation plans and how it will address any findings from the external audit. Interactive is only required to assist the development of the remediation plans, and has no liability to the Customer if the auditor is not satisfied with the Customer's remediation plans.

3 Supply Chain Cyber Risk Assessment

This Service Type applies to Engagements for a Supply Chain Cyber Risk Assessment.

3.1 Interactive will assist the Customer to assess cyber security risks posed by the Customer's third parties ("Supply Chain Cyber Risk Assessment"). The intention of this Service Type is to enable the Customer to make informed information security decisions on its supply chain.

3.2 The Customer will provide Interactive with copies of any written documentation that supports the services that the third party provides to the Customer for Interactive to assess.

3.3 Interactive and the Customer will assess the level of cyber risk posed by each third party based on: (1) the criticality of the third party services to the Customer; and (2) the sensitivity of the information that the third party has, or may have, access to during the third parties engagement with the Customer. Interactive and the Customer will agree and assign a risk rating of low, medium or high to the third party.

3.4 After the tasks set out in item 3.3 are completed, Interactive will perform the following activities:

(a) If a third party is assessed as low risk, Interactive will issue the third party with a short questionnaire about their security controls, review their answers and provide written recommendations to the Customer.

(b) If a third party is assessed as medium risk, Interactive will issue the third party an extensive questionnaire about their security controls, review their answers and provide written recommendations to the Customer.

(c) If a third party is assessed as high risk, Interactive will perform a risk-based audit, which consists of interviewing third party staff and/or reviewing third party policies, procedures and processes against the relevant compliance requirements and cyber risks and provide written recommendations to the Customer.

3.5 The Customer is responsible to ensure that the relevant third party completes any questionnaire provided to it by Interactive. If a third party fails to complete the questionnaire, Interactive is not in breach of its obligations under this Agreement and the Customer remains obligated to pay the Service Fees.

3.6 Interactive will rely on the third party's answers and is not liable for any recommendations Interactive makes based on the third party responses.

4 IT System Cyber Assessment

This Service Type applies to Engagements for an IT System Cyber Assessment.

4.1 Interactive will assist the Customer to understand the cyber risks of the IT System(s) in scope ("IT System Cyber Assessment"), by assessing the confidentiality, integrity and availability risks associated with using the IT System(s) in scope as detailed in the Cyber Security Plan.

4.2 This Service Type consists of the following:

(a) review the type and sensitivity of information in scope;

(b) assess the business processes supported by the IT System(s) and data flows;

(c) perform access reviews, and assess the roles and responsibilities and appropriateness of access;

(d) assess the information security risks relating to all of the above; and

(e) prepare a report that details the information security risks identified during the assessment and sets out the recommendations made by Interactive ("IT System Cyber Assessment Report").

5 ISMS Maintenance

This Service Type applies to Engagement for a ISMS Maintenance.

5.1 Interactive will assist the Customer to maintain its information security management system (ISMS) ("ISMS Maintenance").

5.2 Interactive will perform one or more of the activities set out below based on the scope agreed between the parties:

(a) assess changes to the organisation and the potential impact on cyber risks;

(b) review the effectiveness of controls;

(c) collect and report on security metrics;

(d) facilitate management review meetings and other information security meetings;

(e) preparation of board reports on cyber risk and audit results;

(f) provide information on the changing cyber security threat landscape, including details on cyber-attacks which have occurred in other organisations and learnings from these cyber incidents;

(g) provide recommendations on how to address audit findings, gap assessments and treatment plans;

(h) review and provide recommendations on security awareness training initiatives; or

(i) perform redline mark-ups on policies, procedures and other information security documentation.

Schedule 2 Cyber Security Plan Template

This Cyber Security Plan is dated the last date on which this document is executed

Between

Interactive Pty Ltd **("Interactive")**

ABN: 17 088 952 023
461 Williamstown Road
Port Melbourne Vic 3207

and

[insert name] Pty Ltd **("Customer")**

ABN [Insert No]
[insert address]
[insert address]

1. The parties entered into a CMS SOW commencing on [insert date].

2. This Cyber Security Plan sets out the details of the agreed plan and the Service Days and Service Fees. Once signed, the Cyber Security Plan is incorporated into the CMS SOW. Any terms defined in the CMS SOW have the same meaning in this Cyber Security Plan.

3. Contract Details:

Amount of Service Days	[How many days during the Individual Term will Interactive perform the Services]
Type of Security Manager Services ("Service Type")	[list Service Types to be provided during Individual Term]
High Level Description of required scope	[insert high level description of scope]
Approximate Dates	[insert the agreed dates for the performance of the Services]
Service Fee	[Services Days x Service Fee]

*The Approximate Dates for the performance of the Services may be altered by agreement in writing.

EXECUTED as an Agreement

Signed for and on behalf of **the Customer** by:)
)

_____
Signature of authorised person

_____ _____
Date of signing Name (print)

Signed for and on behalf of **Interactive** by:)
)

_____
Signature of authorised person

_____ _____
Date of signing Name (print)