MASTER SERVICES AGREEMENT

SERVICE DESCRIPTION

SERVICE DESCRIPTION: DEFEND CYBERSECURITY OFFICE (CSO)

PART A – DESCRIPTION

DEFEND Cybersecurity Office (CSO) is a monthly subscription-based service that assists in the establishment, governance, and running of an effective cybersecurity practice within your organisation, aligned to mutually agreed industry standards and the DEFEND Cyber 7 Framework. The day-to-day provision of the CSO service to you is by DEFEND Limited, as subcontractor for One New Zealand.

CSO provides a pool of committed monthly hours headed up by a Senior Cybersecurity Consultant supported by the wider DEFEND team. This commitment allows DEFEND experts to be involved in a 'business as usual' while leveraging DEFEND's cybersecurity knowledge base, policies, frameworks, and IP.

PART B – OPTIONS & INCLUSIONS

OPTIONS			
	Foundational	**Enabled**	**Optimised**
Hours per month A pool of committed hours led by a Senior Cybersecurity Consultant, supported by the Head of Consulting. Hours are interchangeable with suitable specialist individuals.	16	32	64
INCLUSIONS			
Virtual Chief Information Security Officer (vCISO) This role is filled by an experienced cybersecurity consultant who assists with the development and implementation of the customer's cybersecurity programme.	Advisor	Champion	Leader
Cybersecurity Programme Governance Helps plan and set up a measurable programme, directing and driving strategic initiatives and continuous improvement in cybersecurity.	Attend Meetings	Proactive Support	Actively Manage
Cybersecurity Framework Helps to inform and establish a cybersecurity framework, while adopting a continual, structured programme of work with measurable and targeted initiatives. This could be based on the NIST Cybersecurity Framework with all the ISO27001 controls mapped into it.	Advise	Maintain	Own
Cybersecurity Steering Committee Able to set up a cybersecurity governance model, defining roles and responsibilities, and supporting charters. The Steering Committee also works to reflect the customer's strategy into the cybersecurity strategy and roadmap.	Attendee	Member	Chair
Executive Briefings Provides targeted Executive briefings on the current threat landscape, specific cybersecurity topics, or themes (as requested).	One-off as requested (Charges apply)	Annual	Bi-Annually

Cybersecurity Reporting & Dashboard Develop and help populate a dashboard reporting on both operational and strategic metrics, and changes in the internal and external threat landscape.	Quarterly	Monthly	Monthly with enhanced metrics
Incident Management Define incident response plans and playbooks to enable the customer to identify and respond to key threats. Supported by external specialists on a reasonable endeavour's basis.	Provide Guidance	Assist Investigation	End to end Oversight
Cybersecurity Policies & Standards Able to develop security policies and standards that are 'right sized' for the customer. Able to support the communication, adoption, and compliance reporting against set standards.	Review	Update	Produce
Cybersecurity Strategy & Architecture Able to support the definition of cybersecurity architecture in line with the cybersecurity strategy to address identified risks and capabilities requirements.	Assist	Maintain	Produce
Financial & Capital Management Able to help scope and estimate security initiative costs feeding into overall cybersecurity investment plans.	Advise	Report	Manage
Risk Management. Able to develop a cybersecurity risk methodology to identify, analyse, evaluate, and manage risks based on the customer's cybersecurity threats.	Maintain Register	Implement & Maintain Processes	Define & Deploy Strategy, Framework & Processes
Best Practice Guidance An experienced practitioner provides guidance and advice on cybersecurity industry best practice.	✓	✓	✓
Technology/Service Evaluation & Assessment Able to review, assess and evaluate proposed technology or services. Provide vendor agnostic recommendations based on the best fit based on customer requirements.	✓	✓	✓
Point of contact for any cybersecurity queries Subject matter expert(s) for any cybersecurity related queries.	✓	✓	✓
Cybersecurity Awareness Assess the current state of the customer's cybersecurity awareness, to develop a cybersecurity awareness plan and education/testing schedule	Briefing	Training	Training
Policy Exemption Assessment & Recommendation Able to review and provide a risk assessment for a customer-requested security policy requirement exemption.	Advise	Advise & recommend	Advise, Recommend & Approve
Audit & Assurance	Assist	Manage	Deliver

Assist and can advise on the scope of penetration testing or audit. Help interpret results and provide responses including mitigation plans and response.			
Change Advisory Board Able to attend a change advisory board (CAB), to work towards security outcomes. Can act as an approval authority on behalf of the security function.	Process Guidance	As requested	Attend
Access Management Able to review and approve any access requests and is able to define and operate a regular access review process.	As requested, (Charges apply)	Provide guidance	Manage & Authorise
Vulnerability Management Able to define and support the customer's vulnerability management operation and process. The security practitioner is able to support or lead the process around the identification of vulnerabilities and to guide the customer on assessing its potential impact and possible mitigation options.	As requested, (Charges apply)	Review Reports	Proactively Manage

PART C – SERVICE CONDITIONS

1. 1 The CSO service is based on a minimum 12-month term

1. 2 Early termination charges apply

1. 3 All necessary access controls will be provided

1. 4 Access to your physical offices will be provided as required

1. 5 The engagement will commence at a mutually convenient time

1. 6 You will provide remote access to information and communication capabilities

1. 7 You will make available any required system or information

1. 8 You will inform (or authorise us to inform) all relevant parties of the activities being carried out by DEFEND under your authorisation, including any key third parties

1. 9 Travel and disbursements will be agreed prior and charged at cost if required

1. 10 You will be billed the fixed fee for the month regardless of hours consumed (caveat is that any hours above allocated hours per month will be billed at T&M)

1. 11 Allocated hours can be used as above or in the event any unexpected items are discovered and will be identified on a priority basis by the Senior Cybersecurity Consultant.

1. 12 You may request an additional number of hours on a given month over and above what is outlined in this Service Description on a time and materials basis

1. 13 The CSO service is provided during normal business hours on Business Days

1. 14 The CSO service does not offer guaranteed protection from internal, or external Cyber-attacks and risks

1. 15 The CSO service does not provide an incident response team, but assistance may be provided on a reasonable endeavour's basis.