Specific Service Terms – C1 Cyber Security – Monitor, Detect and Advise Service

Calibre One Pty Ltd ABN 87 160 457 090

(Calibre One)

Table of Contents

Specific Service Terms - C1 Cyber Security – Monitor, Detect and Advise Service

1. ABOUT THESE SPECIFIC SERVICE TERMS

1.1 These are the Specific Service Terms – C1 Cyber Security Monitor, Detect and Advise part of the Agreement between Calibre One and the Customer.

1.2 This Agreement is comprised of our General Service Terms (including Schedules to the General Service Terms), these Specific Service Terms – C1 Cyber Security - Monitor, Detect and Advise, and any other Specific Service Terms applying to the Customer for the Services selected in the Scope of Works.

1.3 Calibre One has presented and the Customer has accepted a Scope of Works which includes the provision of C1 Cyber Security – Monitor, Detect and Advise Service (***Cyber Security Service***) to the Customer's Business for its Information Technology requirements. The Scope of Works is for the provision of the Cyber Security Service (and any other services or things as set out in the Scope of Works) and has been prepared based upon any inspection by Calibre One of the Information Technology used by the Customer in the ordinary course of the Customer's Business conducted at the Customer's Premises.

1.4 The Customer warrants that before this Agreement is entered into it has given full and complete disclosure to Calibre One of all its needs and requirements in respect of Information Technology for its Business and Calibre One entered into this Agreement in reliance on that disclosure.

1.5 Calibre One and the Customer have entered into this Agreement to set out the terms on which Calibre One will provide the Cyber Security Service for the purpose of protecting the Customer's Information Technology systems and assets.

2. C1 CYBER SECURITY - MONITOR, DETECT AND ADVISE

What is C1 Cyber Security – Monitor, Detect and Advise

2.1 The Cyber Security Service is a monthly subscription program with initial setup Fees and occasional ad-hoc Fees consisting of the following key elements:

(a) Onboarding and Shaping Up

(i) The onboarding and shaping up process is designed to bring the Customer's Microsoft Office 365 licensed software (***Tenancy***) to a higher level of security. To measure this success we use the in-built Microsoft Office 365 Scorecard System to generate an overall security score for your Microsoft Office 365 software. This will provide a percentage score from a maximum possible of 100% - for example 75% (pretty good) or 11% (really bad).

(ii) Our onboarding process is designed to bring your Tenancy to a minimum 75% security score for your specific environment. In the above example the 75% would be acceptable while the lower figure is not.

(iii) This figure is an evolving score and changes over time as Microsoft introduce new features and threats change.

(iv) Future monitoring of this score and adaptation of your Information Technology environment is one of the variables the Cyber Security service monitors.

(v) Calibre One may choose to suspend provision of security services to any Tenancy not meeting minimum acceptable Microsoft score values as determined by Calibre One in its discretion.

(b) Monitor, Detect and Advise

(i) This component comprises a suite of essential monitoring actions by Calibre One that will alert us to suspicious or malicious activities within your Tenancy.

Some are designed to detect ongoing and persistent external threats, others are designed to mitigate and advise in the event your Tenancy is compromised. This provides essential coverage and then a speedy initial response to cyber security problems which are detected.

(ii) All actions required to triage and respond to an immediate threat are included in the Cyber Security Service and covered by the monthly subscription Fees. Follow up and subsequent investigation work are not included in the standard Cyber Security Service and will be subject to Fees additional to the monthly subscription fees which are to be agreed between Calibre One and the Customer.

(c) Ongoing Reviews, Audits and Risk Assessments

(i) Essential to any cyber security program is ongoing monitoring and assessment of the program itself. Cyber security risks are constantly changing so the Customer needs to regularly review its policies, practices and procedures against the evolving risks. Our Cyber Security Service can provide a bi-annual, or annual scheduled risk assessment reviews, and audits to ensure you remain compliant. The cost of this service is not included in the monthly subscription Fees and will be subject to additional Fees to be agreed between Calibre One and the Customer.

Eligibility

2.2 The Cyber Security Service is available only to Calibre One business and government Customers with an active billing Calibre One or Telstra account number, and the Customer agrees it will maintain an active billing Calibre One or Telstra account number at all times throughout the Term.

2.3 The Customer must be using Microsoft Office 365 as their email platform and the Customer agrees it will maintain an active Microsoft Office 365 Tenancy and associated software licenses as required to operate it, for the Business, at all times throughout the Term.

2.4 Each subscription to the Cyber Security Service can only be used by the nominated Business as referred to in the Scope of Works or as otherwise agreed in writing. The Customer will need to acquire from Calibre One a separate subscription for each Business that uses the Cyber Security Service if the Customer wants to use the Cyber Security Service for multiple Businesses.

2.5 You must not allow any other person or Business to access or use the Cyber Security Service other than the Business nominated in the Scope of Works.

RocketCyber

2.6 The Customer acknowledges and agrees that Calibre One will need to download RocketCyber software onto any Customer's desktop or laptop PC, and virtual or physical server to enable Calibre One to provide the Cyber Security Service and the Customer will be responsible for the associated data and usage charges. The software licence cost for the RocketCyber software is included in the monthly subscription Fee payable by the Customer to Calibre One in connection with the Cyber Security Service.

2.7 The Customer acknowledges and agrees that for Calibre One to provide the Cyber Security Service that each user must maintain a minimum Azure Active Directory Premium P1 active license in your Tenancy, and you agree that you will maintain that, at your own cost, at all times throughout the Term.

2.8 You will not be provided with credentials or access to the RocketCyber software unless agreed to in writing by Calibre One. You must provide Calibre One with reasonable assistance (including but not limited to, passwords to your Information Technology systems and devices) where it is required by us for the purposes of providing you with the Cyber Security Service.

2.9 Calibre One may use other Third Party support providers and suppliers in order to provide the Cyber Security Service to you.

2.10 Calibre One does not warrant or guarantee that access to RocketCyber will be continuous or fault-free.

3. CYBER SECURITY SERVICE FEATURES

Cyber Security Service

3.1 The Cyber Security Service provides access to the Calibre One Business Cyber Security Services helpdesk for assistance with the Cyber Security Services listed in the table in clause 3.2.

3.2 The core features of the Monitor, Detect and Advise part of the Cyber Security Service as outlined in clause 2.1(b) are listed in the following table:

Alert Type	Description of potential attack
Suspicious Logins	This detection system identifies that users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses may be involved in malicious activities, such as Botnet C&C software attacks, and may indicate a compromised account.
Impossible Travel	This detection system identifies two user activities (in a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials. This detection uses a machine learning algorithm that ignores obvious "false positives" contributing to the impossible travel condition, such as Virtual Private Networks and locations regularly used by other users in the organisation.
Activity From Infrequent Country	This detection system profiles your Information Technology environment and triggers alerts when activity is detected from a location that was not recently or never visited by the user or by any user in the organisation. Detecting anomalous locations necessitates an initial learning period of 7 days, during which the system does not alert on any new locations.
Brute Force Attacks	This detection system generates an alert when an excessive volume of login attempts to an account is detected.
Suspicious Email Volume detected	This detection system generates an alert when someone in the Customer's Business has sent more email than is allowed by the outbound spam policy. This is usually an indication the user is sending too many emails, or that the account may be compromised. This system has a medium severity setting. If an alert is generated by this system it is a good idea to check whether the user email account is compromised.
User restricted from sending email	This detection system generates an alert when someone in the Customer's Business is restricted from sending outbound email. This typically results when an email account is compromised, and the user is listed on the Restricted Users page in the Security and Compliance Centre.
Creation of Forwarding Rules	This detection system generates an alert when someone in the Customer's Business creates an inbox rule for their mailbox that forwards or redirects messages to another email account. This system only tracks inbox rules that are created using Outlook on the internet or Exchange Online PowerShell.
Creation of Suspicious Email Rules	This detection system generates an alert when someone in the Customer's Business creates an inbox rule for their mailbox that performs an action deemed as suspicious.

3.3 We may liaise with Third party Support providers and suppliers on your behalf to provide the Cyber Security Service.

Limitations

3.4 The Cyber Security Service is not available for some Information Technology devices, software and operating systems, and the Customer is responsible for ensuring that its Information

Technology systems are compliant with all eligibility requirements to receive the Cyber Security Service as set out in these Specific Service Terms.

3.5 Except for the RocketCyber agent software which Calibre One provides to the Customer, the cost of any other software and hardware is not included in the monthly subscription Fees for the Cyber Security Service. The Customer is responsible for any data and usage charges on its Information Technology system associated with the Cyber Security Service.

3.6 The Cyber Security Service does not include the remediation works required as a result of any malicious activity. We will advise you of any such attack and the remediation works can either be performed by you, a Third Party service provider, or us for a Fee to be agreed and which will be additional to the monthly subscription Fee.

3.7 The Customer is responsible for the costs and charges of remediation works carried out by any Third Party service provider. The Third Party costs and charges are not included in the monthly subscription Fee for the Cyber Security Service, and you will be billed separately as per your own arrangement with any Third Party service providers.

3.8 The monthly subscription Fee does not include:

(a) the replacement or physical repair of hardware;

(b) the supply of any software other than the licence fees for RocketCyber software as included in the monthly subscription Fee; or

(c) the supply of professional services beyond standard technical support and advice covered by the Cyber Security Service.

3.9 Calibre One will endeavour to accommodate any reasonable requirements of the Customer in relation to the scope, time and location for provision of the Cyber Security Service but Fees in addition to the monthly subscription Fees may apply to accommodate specific Customer requests with such additional Fees to be notified and agreed in advance.

3.10 We do not guarantee any resolution or response timeframes for service requests or remediation work requests.

3.11 In the instance of attacks on your Information Technology by any encryption based malware or other destructive malware we cannot “unlock” or retrieve data on affected drives.

3.12 Following any security reviews, audits or risk assessments outlined in clause 2.1.3, we will provide you with a report and recommendations. We do not guarantee, represent or warrant that any such report is complete or free from errors or that the recommendations contained in it will produce particular results, lead to a particular outcome or protect against all risks and vulnerabilities. The Customer agrees that Calibre One is not liable for any loss or damage suffered by you or any party as a result of the review, audit, assessment, report or recommendations, even if arising from Calibre One's negligence. This includes but is not limited to, loss of or damage to profits, income, revenue, use, production, anticipated savings, business, contracts, commercial opportunities or goodwill. You agree that you are best placed to review any recommendations made by Calibre One in any security review, assessment, or audit, as they will or may impact you, and you must satisfy yourself as to their appropriateness for your needs.

3.13 You must have full authorisation (including from relevant Third Parties) at all times as required for our personnel to perform the Cyber Security Service, including by obtaining any prior written approval required for our personnel to monitor, scan or access any of your Information Technology (including systems hosted, managed, owned or under the control of a Third Party). In performing our obligations to you, we rely on the timeliness and accuracy of the information and assistance you give us (including by you obtaining all necessary Third Party consents, and approvals required from any Third Party that supplies you with web hosting, IT support, cloud computing facilities, firewall management, or other services).

3.14 You are responsible for backing up the data in your Information Technology system before we provide the Cyber Security Service to you. You acknowledge and accept the risk that the supply of the Cyber Security Service may result in or cause interruptions, loss or damage to you and your Information Technology systems data, and that we do not separately back-up any of your data to avoid potential data loss. You agree that to the fullest extent permitted by Law, we have

no liability to you or any of your Related Entities as a result of such interruptions, loss or damage.

3.15 To the extent that you are giving Calibre One access to Confidential Information of other individuals as part of providing the Cyber Security Service, you must ensure that you have obtained all privacy consents required from those individuals to enable us to perform the Cyber Security Service.

Fair Use

3.16 You must not use the Cyber Security Service or let the Cyber Security Service be used:

(a) to commit an offence or breach any laws, standards or codes applicable to the Cyber Security Service;

(b) to infringe the intellectual property rights or other rights of any person;

(c) for resale to another person or organisation; or

(d) in a manner that is excessive or unusual.

3.17 If your access to the Cyber Security Service exceeds three times the average of all users of the Cyber Security Service in any monthly period which will constitute excessive usage, we may contact you to discuss your usage of the Cyber Security Service, and if your usage continues, in the opinion of Calibre One to be excessive in the following monthly period, we may warn you that your Cyber Security Service may be terminated, and if your usage continues, in the opinion of Calibre One to be excessive for a third consecutive monthly period, then we may immediately terminate this Agreement so far as it covers your Cyber Security Service by giving you written notice.

Adverse Use

3.18 You must not use the Cyber Security Service in a manner which adversely affects another customer's use of the Cyber Security Service. If we have reasonable grounds to believe that this is occurring, we may suspend your Cyber Security Service without notice until we are satisfied that this is no longer occurring.

Your obligations

3.19 So that Calibre One can provide the Cyber Security Service to you, you must at your cost and without delay provide us with:

(a) all complete and accurate information (including technical data, consents and all other information); and

(b) cooperation and assistance,

which we may reasonably request from you from time to time.

4. PLANS AND CHARGES

4.1 Adhoc Fees and a monthly subscription Fee apply to the Cyber Security Service as follows:

Key Element	Charge Type	List Price	Minimum Term
Onboarding and Shaping Up	Adhoc (Upfront)	See Scope of Works	n/a
Monitor, Detect and Advise	Monthly	See Scope of Works	12 months
Ongoing Reviews, Audits and Risk Assessments	Adhoc (Ongoing)	See Scope of Works or, alternatively as may be agreed	n/a

4.2 The monthly subscription Fee payable by the Customer for the Cyber Security Service will continue to apply until the end of the period of subscription to your Cyber Security Service which shall continue throughout the Term unless cancelled or terminated earlier under the terms of this Agreement. The Customer may cancel the Cyber Security Service at any time by giving 3 months' notice in writing to Calibre One, in which event this Agreement so far as it relates to the Cyber Security Service will be terminated at the end of that 3 month notice period and the

full monthly subscription Fees will apply during that 3 month notice period as well as any other Fees payable in relation to that period.

4.3 Calibre One may at its discretion discontinue the Cyber Security Service or make changes to our Fees at any time. We will give you 30 days' advance written notice of any increase in our Fees, and if the change, other than an adjustment to our fees in accordance with movement in a consumer price index as provided for in the General Service Terms, is unacceptable to the Customer, you can terminate this Agreement, so far as it relates to the Cyber Security Service, by giving us notice in writing which notice may be given by you at any time during the 30 days' advance written notice of the increase in our Fees given by Calibre One to you (if you do not give notice terminating within that 30 day period you will be deemed to have accepted the change to our Fees at the end of that period).

4.4 The monthly subscription Fee for the monitor, detect and advise component of the Cyber Security Service is per user, plus per Information Technology device. The number of users and devices as at commencement of the Cyber Security Service is as set out in the Scope of Works. Calibre One reserves the right to adjust the number of users and devices for the purpose of calculating the monthly subscription Fee based on counts observed, and information provided by the Customer. The Customer will update Calibre One by providing it with details in writing of any changes in the number of users and devices in its Business within 14 days of any change.

5. GENERAL CONTRACT TERMS

Exclusivity

5.1 Calibre One will throughout the Term be the exclusive provider to the Customer of all those services of the type comprised in the Cyber Security Services. This is an essential term of this Agreement.

5.2 The Customer must not, without the express prior written approval of Calibre One obtained in advance, interfere with, alter or change the RocketCyber software and related technology or permit any person other than Calibre One to interfere, alter or change it.

Modifications to Specific Service Terms

5.3 Once these Specific Service Terms have been agreed and this Agreement entered into, matters contained within these Specific Service Terms may, unless expressly provided otherwise, only be adjusted from time to time by mutual Agreement in writing between Calibre One and the Customer.