OUR CUSTOMER TERMS
TELSTRA BUSINESS CYBER SECURITY SERVICES

Contents

OUR CUSTOMER TERMS
TELSTRA BUSINESS CYBER SECURITY SERVICES

1 ABOUT TELSTRA BUSINESS CYBER SECURITY SERVICES

1.1. The following terms and conditions will apply to your use of Telstra Business Cyber Security Services.

1.2. Unless you have entered into a separate agreement with us which excludes them, the General Terms section of Our Customer Terms also apply.

1.3. If the General Terms for Business and Government customers are inconsistent with something in the Telstra Business Cyber Security Services, then this Telstra Business Cyber Security Services section applies instead to the extent of the inconsistency.

1.4. If a provision of this section gives us the right to suspend or terminate your service, that right is in addition to our rights to suspend or terminate your service under the General Terms for Business & Government.

2 TELSTRA BUSINESS CYBER SECURITY SERVICES

What is Telstra Business Cyber Security Services?

2.1 Telstra Business Cyber Security Services is a month to month subscription service (**Subscription**) and includes standard technical support for the Subscription Services listed in this section. This includes, but is not limited to, assistance with cyber security related IT issues such as business continuity, assistance with software installation and upgrades, networking and cloud application support and advice and coaching for supported cyber security business applications and technology.

2.2 We will deliver the Subscription Services for Telstra Business Cyber Security Services remotely, through a variety of service delivery technologies and agents and is available online or via telephone 24 hours a day, 7 days a week.

Eligibility

2.3 Telstra Business Cyber Security Services is available to small business customers with an active billing account number.

2.4 Each Subscription can only be used for the nominated business. If you wish to use Telstra Business Cyber Security Services for another business, you will need to acquire from us a separate Subscription for each business.

2.5 You must not provide, or assist with the provision of, your Subscription to another person.

LogMeIn

2.6 You acknowledge that Telstra will need to download LogMeIn software onto your computer to enable us to provide the Subscription Services and you will be responsible for the data and usage charges.

2.7 You will be provided with credentials for the LogMeIn. You must provide Telstra with reasonable assistance (including but not limited to, passwords to your systems and

devices) where it is required by us for the purposes of providing you with assistance for the Subscription Services.

2.8 By using the LogMeIn app, you consent to us accessing your device's camera and microphone to provide or deliver the Subscription Services remotely. You will prompted by us before we do so. You must inform anyone else who is present during the interaction that the interaction may be recorded.

2.9 We may use other third party support providers and suppliers (such as Belarc, Inc) in order to provide the Subscription Services to you (without disclosing this to you).

2.10 We cannot guarantee that access to the LogMeIn will be continuous or fault-free.

3 SERVICE FEATURES

Subscription Services

3.1 The Subscription provides access to the Telstra Business Cyber Security Services helpdesk for assistance with the services listed in the clause below (each a **Subscription Service**).

3.2 The Subscription Services are listed below:

Telstra Business Cyber Security Services	**Description of available services**
Security & Protection	○ Cyber Security On-Boarding service call and over the phone assessment to help protect your business (maximum one per month and 4 in a 12 month period) ○ Cyber Security Health check report issued after assessments to help protect your business. ○ Setup of your anti-virus software ○ Settings and privacy setup ○ Help with Microsoft Office recovery ○ Support for malicious software removal ○ Network security support/guidance and configuration ○ Security – Ability to assist with setup and configuration of firewalls, end point protection, backup and recovery plan ○ Servers - Ability to diagnose issues with servers and assist with remote configuration ○ Email updates on security advice (this feature is being removed on and from 30 September 2021)
Back-up and recovery	○ Setup, assistance and advice with: • Cloud storage • Data storage (Transfer limits should not exceed 50GB) • Support with data backup • Data archiving

Devices, Apps & Hardware	○ Software, mobile, laptop, tablet cyber security checks on demand to help protect your business ○ Device operating system recovery where possible ○ Modem and Router security configuration ○ Support with security devices (cameras etc.)
24/7 support	○ Access to a cyber security specialist over the phone and via online chat from Townsville, Australia, 24 hours a day, 7 days a week
Telstra Internet Protection Mail and Telstra Internet Protection Web	○ Access to Telstra Internet Protection Mail and Internet Protection Web (**Internet Protection Services**) to help guard against a range of wen and email related security risks ○ Preconfigured web and email policies ○ Access to a policy management and reporting portal ○ Assistance with setup, configuration and reporting

3.3 We may liaise with third party support providers and suppliers on your behalf to provide Subscription Services.

Limitations

3.4 Telstra Business Cyber Security Services is not available for some devices and software and operating systems.

3.5 Except for any Internet Protection software we provide to you, the cost of any software/hardware is not included in monthly charge for the Subscription. You are responsible for any data and usage charges.

3.6 If applicable, you will be given prior notice of relevant charges from third party support providers and the services will be provided by them. You are responsible for these charges, they are not included in your monthly charge for your Subscription, and you will be billed separately for them as per your arrangement with those third party providers.

3.7 The scope, time, and location of Telstra Business Cyber Security Services will be agreed upon prior to delivery. The scope of the services can be changed prior to delivery. Additional delivery charges may apply when connecting your Telstra services and we will advise you of these in advance.

3.8 We do not guarantee resolution timeframes for service requests.

3.9 In the instance of Encryption based malware we cannot “unlock” or retrieve data on affected drives.

3.10 In store or on-premises support is not included with this subscription.

3.11 The Subscription charge does not include:

(a) the replacement or physical repair of hardware;

(b) the supply of any additional software; or

(c) the supply of professional services beyond standard technical support, advice and coaching (for example, website building, software migrations or development work).

3.12 Following a security assessment, we will provide you with a report and recommendations. It provides advice only, and we do not guarantee, represent or warrant that that it is free from errors or the recommendations contained will produce particular results, lead to a particular outcome or protect against all risks and vulnerabilities. We are not liable for any loss or damage suffered by you or any party as a result of the assessment, report or recommendations. 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 the recommendations made within as they will or may impact you, and you must satisfy yourself as to their appropriateness for your needs

3.13 You must not rely upon the assessment or the report as an alternative to advice from a qualified professional and you should ensure you monitor your own practices and investigations. If you have any specific questions, you should consult an appropriately qualified professional.

3.14 You must have full authorisation (including from relevant third parties) for our personnel to perform the Subscription Services, including by obtaining prior written approval for our personnel to monitor, scan or access any of your IT infrastructure (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 for us to perform our obligations to you, including obtaining approvals from any party that supplies you with web hosting, IT support, cloud computing facilities, firewall management, or other services).

3.15 You are responsible for backing up your data before we provide the Subscription Services to you. You acknowledge and accept the risk that the supply of the Subscription Services may result in or cause interruptions, loss or damage to you and your computer systems, networks, websites, internet connections and data, and that we do not separately back-up any of your data to avoid potential data loss. You agree that to the full extent the law allows, we have no liability to you or any party as a result of this.

3.16 You will ensure that a person aged over 18 years is present to provide us with passwords to your computer and systems (as required) and reasonable assistance with using your systems so that we can perform the services.

3.17 You will ensure that any software you use or supply for use in conjunction with a Telstra service is legal and has a valid licence.

3.18 To the extent that you are giving Telstra access to personal information of other individuals as part of providing the services, you must ensure that you have obtained

any necessary privacy consents from those individuals to enable us to perform the services.

Fair Use

3.19 You must not use Telstra Business Cyber Security Services or let the service be used:

(a) to commit an offence or breach any laws, standards or codes applicable to the service or breach our FairPlay Policy (available at https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/consumer/mobilegeneral.pdf);

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

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

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

3.20 If your:

(a) access to the Subscription Services exceeds three times the average of all users of the service in a billing period (excessive usage), we may contact you to discuss your usage of the service;

(b) if your usage continues to be excessive in the following billing period, we may warn you that your service may be terminated; and

(c) if your usage continues to be excessive for a third consecutive billing period, then we may terminate your service.

Adverse Use

3.21 You must not use this service in a manner which adversely affects another customer's use of the service. If we have reasonable grounds to believe that this is occurring, we may suspend your service without notice.

4 INTERNET PROTECTION SERVICES

4.1 The Internet Protection Services do not activate upon being subscribed to Telstra Business Cyber Security Services. To activate, call 13 70 55 or book an onboarding or assessment over the phone to start using Internet Protection Mail and Internet Protection Web.

4.2 The Internet Protection Services provides security features for your email and web traffic.

4.3 We don't promise to:

a) supply the Internet Protection Services without any outages, faults or delays;

b) fix all defects, problems or issues; or

c) detect or block all spam, viruses, malware or other harmful programming. Some legitimate email messages may get identified as spam. We don't

guarantee that the Internet Protection Services or platform will be free from intrusions, viruses, Trojan horses, worms or other similar harmful programming routines.

4.4 You must ensure that the Internet Protection Services are installed and used as per the installation guidelines which we provide and as per our instructions from time to time. The Internet Protection Services may not work on all systems and set-ups. We'll confirm which ones are compatible around the time you apply for the Internet Protection Services.

4.5 We procure the right for you to use software that is part of or needed to use the Internet Protection Services. This is usually on the same terms that our vendor grants such licences. You must comply with (and ensure all your end users comply with), all applicable licence terms at all times.

4.6 Subject to applicable law, we may provide the Internet Protection Services from any hardware or other installation anywhere in the world at our choice. You acknowledge that we may use shared infrastructure to deliver the Internet Protection Services and we don't promise that any installation or any part of it is dedicated to your sole use.

4.7 If we reasonably think that the provision of an Internet Protection Service to you compromises or may compromise the security of the Internet Protection Service or our network (for example due to hacking attempts or denial of service attacks), then we may temporarily suspend the Internet Protection service.

4.8 We'll try and tell you if we temporarily suspend your Internet Protection Services. We'll then try and work with you to with the aim of re-instating the service to you.

4.9 Your Internet Protection Services will be cancelled upon the cancellation of your monthly Telstra Business Cyber Security Service subscription.

4.10 Upon cancelling your Internet Protection Services, if you have configured Internet Protection Mail, you will need to change your email settings back to default otherwise your email service will stop working. You can get assistance with this by calling the Cyber Security team on 13 70 55.

Your obligations

4.11 So that we can provide the Internet Protection Services to you, you must at your cost provide us with:

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

b) cooperation and assistance,

we may reasonably request from time to time

4.12 You must:

a) not falsify, forge or otherwise tamper with any portion of the header or tracking data of any SMTP email message;

b) use the Internet Protection Services in a responsible manner and not allow your email systems to:

(i) act as an open relay;
(ii) send or receive bulk email where such bulk email was initiated by you; or
(iii) originate, send or relay spam or intentionally launch viruses.

4.13 If you breach clause 4.12 we may immediately suspend all or part of your Internet Protection service until you rectify the issue to our satisfaction.

Internet Protection Web

4.14 To use the Internet Protection Web service, you must ensure your external traffic is always directed through the Internet Protection Web service.

4.15 We don't promise that the Internet Protection Web service will function for web traffic that you haven't routed in the way we recommend from time to time.

4.16 You're responsible for configuring your systems to direct external traffic through the Internet Protection Web service.

4.17 You must ensure that your internal traffic (for example traffic to your corporate intranet) isn't directed through the Internet Protection Web service.

Internet Protection Mail

4.18 The Internet Protection Mail service won't scan attachments if the file can't be read or opened (e.g. Zip files or encrypted files where the file can't be read without using a decryption device).

4.19 You must have a registered domain name to use the Internet Protection Mail service.

4.20 You must appropriately configure your domain name system to use the Internet Protection Mail service. On request, we can provide technical information on how to do this.

4.21 The service assurance and network availability targets which apply to the Telstra Internet Direct service don't apply to the Internet Protection Mail service.

4.22 If we detect a rising email queue for your domain, we may test your receiving mail server's ability to receive email and may tell you if this test fails.

4.23 If we can't deliver email to you, then we may try to store your inbound email for up to three days. After this, your emails and web traffic will be deleted from our systems.

5 PLANS AND CHARGES

Subscription Services

5.1 The Telstra Business Cyber Security Services Subscription plan details and monthly charge is:

Option	Helpdesk access	Monthly charge	Minimum term
Telstra Business Cyber Security Services	24 hours a day, 7 days a week	**$80**	A month (month to month subscription)

5.2 Your plan and Subscription charge will continue to apply until you cancel your service. There are no early termination charges, and you may cancel any time but the full monthly fee will apply for the current billing cycle and you will need to pay any charge owing for that billing month.

5.3 There will be no credits for charges already billed in advance.

5.4 Telstra may at its discretion discontinue the service or make changes to the price at any time. We will give you 30 days' written notice where possible.

5.5 In our full discretion, we may decide to offer to waive the monthly charge specified above for a limited time, for example, where your monthly spend on other Telstra services is more than a specified amount per month. If we invite you to take up this offer, this offer applies until removed by us or your spend falls below this amount. Where this occurs we may remove Telstra Business Cyber Security Services from your account but we will contact you before we do so to discuss alternatives.

6 PRIVACY AND ACCESS

6.1 You consent to us contacting you directly for any purpose reasonably related to any Telstra Business Cyber Security Services that you use (for example, to set up and carry out an onboarding call, to set up and carry out Cyber Security assessments, to contact you to obtain feedback or complete a survey in relation to the service).

6.2 You must promptly report any faults or issues with your service to us and provide all reasonable assistance in using your systems.

7 DATA AND CONFIDENTIALITY

7.1 We may share your data with third parties where it is necessary for the resolution of your technical issue or to carry out the Subscription Services.

7.2 Please note that any personal information collected, used and disclosed will be in accordance with our Privacy Statement (available at www.telstra.com.au/privacy/privacy-statement/?red=/privacy/privacy_statement.html)