OUR CUSTOMER TERMS
MANAGED SECURITY SERVICES SECTION

CONTENTS

OUR CUSTOMER TERMS
MANAGED SECURITY SERVICES SECTION

Certain words are used with the specific meanings set out in clause 14 and in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm.

1 ABOUT THIS SECTION

1.1 This is the Managed Security Services section of Our Customer Terms.

1.2 The General Terms of Our Customer Terms also apply to your Services. See section one of the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm for more detail on how the various sections of Our Customer Terms are to be read together.

2 MANAGED SECURITY SERVICES

Our services

2.1 Our Managed Security Services can include design, monitoring and management of your digital and physical assets, depending on which service elements you choose.

2.2 We provide our Managed Security Services by way of shared infrastructure, dedicated infrastructure and virtualised applications, depending on what services you acquire.

2.3 Our Managed Security Services provide Cyber Detection and Response services (**CDR Enterprise**) (formerly "Security Monitoring").

2.4 The details of our Managed Security Services, and the other services we offer, are set out below.

Availability

2.5 The CDR Enterprise terms in this Managed Security Services section of Our Customer Terms only apply to services contracted before 30 August 2024. For CDR Enterprise services contracted or renewed on and from 30 August 2024, please refer to the Cyber Detection and Response Section of Our Customer Terms.

2.6 To provide the Managed Security Services, we need to be able to connect to your device, application or service (as the case may be). We'll tell you when you apply for the Managed Security Services what the minimum connectivity requirements are.

2.7 There are elements of the Managed Security Services that we can only provide if you have certain devices, applications or services. If you don't have the minimum requirements needed for the service you want to acquire, we can't provide that service to you. We'll tell you the minimum requirements on request.

2.8 The Managed Security Services are not available to Telstra wholesale customers or for resale.

3 WHAT IS CYBER DETECTION AND RESPONSE (CDR ENTERPRISE)?

3.1 The CDR Enterprise (formerly "Security Monitoring") service comprises the following services:

(a) logging – this service stores the log and event data we receive from you;

(b) event monitoring, correlation and classification – this service monitors logs and events for Incidents;

(c) incident notification – this service provides notification of Incidents and may include rating of these Incidents; and

(d) if included, Vulnerability Management – this service scans for vulnerabilities in the IT assets that we've agreed with you.

In this clause 3, references to "CDR" are references to "CDR Enterprise" only.

How we provide CDR and what you must do

3.2 We provide the CDR service:

(a) using shared infrastructure and the public cloud, unless we otherwise think it's appropriate to use dedicated infrastructure; and

(b) through a method between your infrastructure and our infrastructure that we will confirm to you on request.

3.3 To receive the CDR service, you must at your own cost:

(a) separately obtain an appropriate carriage service;

(b) ensure the term of that carriage service does not end before the term of your CDR service; and

(c) complete changes to your network and resources as we require from time to time to allow log and event data to be passed to us from your infrastructure to our infrastructure using a means that we require.

3.4 Each element of the CDR service comprises one or more stages, depending on the service:

(a) the first stage is provided on a once-off basis at the start of your service;

(b) the second stage is provided on an ongoing basis during the term, once the first stage is completed; and

(c) the third stage is provided periodically during the term as we think necessary.

Service	**First stage**	**Second stage**	**Third stage**
Logging	Design the network connectivity to our infrastructure. Configure our infrastructure and create the required VPN tunnel to your infrastructure.	Capture your logs and events, often in near real time where we think necessary. Store your log data in a secure environment. Provide access to your log data via the Telstra Security Portal.	N/A
Event monitoring, correlation and	On-board the platform to accept your log and event data.	Correlate and classify your Security Events. Store your Security Events in a	N/A

classification	Apply the default correlation and classification configurations.	secure environment. Provide access to your Security Events via the Telstra Security Portal.	
Incident notification	N/A	Expert assessment of your Incidents. Provide a ticket on your Incident within the Telstra Security Portal.	Automatically alert your nominated contact point when we detect an Incident.
Vulnerability Management ("Premium" service tier only as set out in clause 3.5 below)	On-board to scanning platform and scanning of IP addresses (up to the number specified in your application form). Conduct asset discovery (map) scans. Classify assets. Set up scans for initial reports.	Access to the Telstra Security Portal. Access to scanning reports.	Notify of newly discovered vulnerabilities. Alert if scanners don't respond to configured "heartbeats".

What service tiers are available?

3.5 The features of your CDR service are set out in the table below based on the applicable service tier.

Features	Premium	Premium – ISM Certified
Certified to operate at the "ISM PROTECTED" level	No	Yes
Online log and event retention	Up to 12 months*	Up to 12 months*
Offline log and event retention	Up to 7 years*	Up to 7 years*
Allowed number of notification contacts	Up to 5	Up to 5
Incident notification (includes both event monitoring, correlation and classification and logging services)	Included	Included

Vulnerability Management scanning	Included	Not included
Retention of vulnerability scan reports	7 days	7 days
Retention of raw vulnerability scan data	12 months*	12 months*

* This is a rolling period, after which we may not be able to recover the log event.

3.6 We will allocate up to a total of 10 terabytes of storage for your logs, events and reports (based on the package you choose) as part of the CDR service. You can request additional storage. If we accept your request, we will confirm the applicable charge for that additional storage.

3.7 Once you reach your allocated storage, your oldest log and events we stored will be over-written to store your new incoming log and events from your device. When this happens, the "first in and first out" principle will be applied to your allocated storage.

How do we rate and notify you of Incidents?

3.8 As part of your CDR service, we will rate your Incidents using the following table as guidance:

Incident rating				
Impact / **Urgency**	**Extensive** (Direct / indirect impact on more than 1 critical asset)	**Significant** (Direct / indirect impact on at least 1 critical asset)	**Moderate** (Direct / indirect impact on more than 1 non-critical asset)	**Minor** (Any other identified Incident)
Category 1 (less than 2 hours)	Priority 1	Priority 2	Priority 2	Priority 3
Category 2 (between 2 hours and up to 12 hours)	Priority 2	Priority 2	Priority 3	Priority 4
Category 3 (more than 12 hours and up to 24 hours)	Priority 2	Priority 3	Priority 3	Priority 4
Category 4 (more than 24 hours)	Priority 3	Priority 3	Priority 4	Priority 4

Impact = How severe we think the Incident is on an **asset**.

Urgency = How soon we think the Incident needs to be addressed.

Asset = A device you own on the network that if compromised, could significantly and detrimentally impact your business. Examples of assets are web servers, databases or workstations. With our agreement, you will nominate to us which of your assets are critical or non-critical (and you must act reasonably in doing so). Although we may give you guidance on the categorising of your assets, you're solely responsible for that categorisation.

3.9 We are solely responsible for rating your Incidents. This means that any security issue or attack blocked by another vendor's product or signature, or by your own policy, is not automatically deemed to be an Incident. A ticket will not be created for that issue or event unless we have rated it in a way that requires a ticket to be created.

3.10 You can choose not to receive email or SMS alerts by changing your preferences on the Telstra Security Portal.

What is Vulnerability Management?

3.11 The Vulnerability Management service:

(a) is only available with the "Premium" service tier and is not available with the "Premium - ISM Certified" service tier of the CDR service;

(b) remotely scans IT assets and IP addresses that we've agreed with you, against a list

of known security vulnerabilities; and

(c) is self-service so you can schedule scans, view configurations, and run and download reports via the Telstra Security Portal.

3.12 To obtain the Vulnerability Management service, if we ask you to, you must promptly and at your own cost:

(a) install internal scanners for vulnerability scanning;

(b) configure your systems to allow your assets to be scanned (such as implementation of firewall rule changes); and

(c) comply with our other reasonable requests.

3.13 You are responsible for backing up your data before we provide the Vulnerability Management service to you. You acknowledge and accept the risk that the supply of the Vulnerability Management service 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 and subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we have no liability to you or any party as a result of this.

3.14 You agree that for your Vulnerability Management service:

(a) scan reports show a point in time of your assets at the time of the scan;

(b) your scan uses a list of known vulnerabilities, which is continually updated, and this may impact the currency of your scan reports;

(c) scans don't detect all vulnerabilities or vulnerabilities that are known at the time of the scan;

(d) you're responsible for scheduling scans at appropriate intervals based on your security needs; and

(e) the service doesn't test, exploit, manage, rectify or fix any vulnerabilities or issues - these are your responsibility.

3.15 Given the nature of the service, the service levels and service credits in this section of Our Customer Terms don't apply to your Vulnerability Management service.

3.16 You must:

(a) only use the Vulnerability Management service (and any reports generated) solely for your internal use and to scan assets that you have the legal right to scan;

(b) not scan the assets of a third party; and

(c) not modify, interfere with, transfer, or affect the operation of the Vulnerability Management service in any way.

What optional components are available?

3.17 You may request:

(a) additional log and event storage capacity and retention periods;

(b) services to extract your logs from storage; and

(c) where Vulnerability Management is included, scanning of additional IP addresses above the number specified in the application form as included in your service tier.

If we agree to your request, we will confirm the applicable charges.

How do you access your service?

3.18 You can access your CDR service via the Telstra Security Portal.

3.19 The Telstra Security Portal aims to let you do the following:

Event monitoring, correlation and rating	**Incident notification**	**Vulnerability Management ("Premium" Service Tier only)**
View and track your rated Incidents. Raise a service request to view your archived Incidents. Generate reports on your Incidents.	View expert assessment of your Incidents.	Configure scans. Run reports. View vulnerabilities against assets. View and download reports.

What are the service limitations?

3.20 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we don't promise that the CDR service will correctly detect and identify all:

(a) Security Events or Incidents;

(b) unauthorised access to your network;

(c) viruses;

(d) spam; or

(e) other types of attacks or issues.

3.21 You must promptly tell us if you find limitations or issues with your CDR service.

3.22 You must give us at least 10 business days' notice before any vulnerability or penetration testing occurs to your network (except for scans as part of your Vulnerability Management service).

Term and termination

3.23 When you cancel your CDR service:

(a) we will store your logs for up to 90 days from the date of cancellation (at your expense), unless you tell us in writing that you do not want us to do this;

(b) you may request an extract of your logs during this 90 day period;

(c) you must pay a fee for this extraction and we can confirm this fee on request;

(d) you will not be able to request an extract after this 90 day period; and

(e) your Vulnerability Management service will also be cancelled and we won't retain any scan data or reports.

4 WHAT ARE THE CDR SERVICE LEVELS?

What are the provisioning and change service levels?

4.1 The provisioning and change service level targets are:

Item	Description	Service level target
Provisioning time	Time from when we receive your order until the time the service is provisioned	20 business days
Activation time for adds, moves or changes	Time from when we receive and approve a written request from you until the time when we complete the change	10 business days

The provisions of this clause 4 apply to CDR Enterprise, and references to "CDR" in this clause 4 should be read accordingly.

4.2 Our provisioning and change service level target assume the following:

(a) timing begins when we receive your written order or request with all fields fully and accurately completed;

(b) we have already accredited and approved all of your data sources that we need to provide the CDR service to you;

(c) timing excludes any time waiting for you to provide information we need to progress your order or request; and

(d) excludes any time needed to alter or prepare your network, devices or other resources in connection with the order or request.

What are the service quality service levels?

4.3 The service quality service level targets are:

Item	Description	Incident priority	Service Level Target
Incident rating time	Time from when the CDR platform receives a Security Event to the time an Incident is rated in the Telstra Security Portal	1	15 mins
		2	30 mins
		3	60 mins
		4	180 mins
Incident notification time	Time from when an Incident is reported by the agreed method below	1	15 mins
		2	30 mins
		3	N/A
		4	N/A
Incident notification method	The method we use to notify your nominated contact person of Incidents	1	Portal + email + phone call
		2	Portal + email + Phone call
		3	Portal
		4	Portal
Service management	How often we contact you about your CDR service	NA	Monthly

What is the service availability service level?

4.4 The monthly service availability service level targets are:

Item	Description	Service level target
Availability of the Telstra Security Portal for the CDR service	Calculated per calendar month	99%
Availability of the CDR platform (excluding the Telstra Security Portal)	Calculated per calendar month	99%
The service level is calculated as follows: Availability = {[(A – B) – C / (A – B)] x 100} A = Total number of hours in the month. B = Number of hours in a planned outage period in the month. C = Number of outage hours for the CDR platform in the month.		

What is the fault reporting service level?

4.5 The fault reporting service level targets are:

Item	Description	Service level target
Initial response time for faults reported via the service desk	Measured from when you report a fault to when we respond	Priority 1: 30 mins Priority 2: 60 mins Priority 3: 120 mins Priority 4: 240 mins
Initial response time for system generated faults	Measured from when you report a fault to when we respond	Priority 1: 15 mins Priority 2: 30 mins Priority 3: 60 mins Priority 4: 120 mins
Service restoration	Measured from when a fault is reported to when the fault is resolved	Priority 1: 95% restored (or work around) in 6 hours Priority 2: 95% restored (or work around) in 12 hours Priority 3: 95% restored (or work around) in 24 hours Priority 4: 95% restored (or work around) in 72 hours

Progress updates	Measured from when we last updated you on the issue	Priority 1: every 1 hour Priority 2: every 4 hours Priority 3: every 12 hours Priority 4: every 24 hours

What service credits may be available?

4.6 If we do not meet the service level targets in this clause 4, you can request a service credit. You must do this by telling us in writing within 30 days from the date that we did not meet the applicable service level.

4.7 After we receive your request under clause 4.6, we will confirm with you if a service credit is due (and we will act reasonably in doing so). The following applies to your service credits:

(a) if a service credit is due, we will rebate you an amount equal to 10% of your monthly charge for the impacted CDR service;

(b) in any given calendar month, your entitlement to service credits is capped to an amount equal to 20% of your monthly charge for the impacted CDR service;

(c) you cannot receive more than one service credit in any 24 hour period, regardless of the number of service legal target failures in that period; and

(d) we endeavour to meet the service level targets in this clause 4 and your request for the applicable service credit is your only remedy for our failure to do so.

4.8 Service credits don't apply where the failure to meet the service level target is affected by:

(a) a fault with your product, service or resource that is caused by you or a third party;

(b) any third party act or omission;

(c) the cutting of cable or fibre which is needed to provide your product or service;

(d) interference or damage to our equipment or network by you or by a third party;

(e) a fault beyond our network boundary point or with your equipment or resources (unless we have specifically agreed in writing to support these things); or

(f) any other cause beyond our reasonable control (including acts of God, industrial disputes of any kind, lightening, fire, earthquake, storm, flood, government restriction, determination of any government or regulatory body, determination of any court of law or any such similar event).

5 OPTIONAL SERVICES

5.1 Managed Security Services include optional services that you can ask us to provide to you.

5.2 If you do ask us to provide any optional services, we use reasonable efforts to comply with your request. We record the detail of your optional services in your application form.

5.3 If additional charges apply for these optional services, we'll tell you what they are when you apply for the optional services, and you have to pay the additional charges on top of the charges for the core components of the logging service.

6 EQUIPMENT

6.1 We can only provide the Managed Security Services if you have equipment that we support. If you don't have that equipment, you can buy or rent it from us.

6.2 We deliver the equipment that you rent or purchase from us to the address you nominate. You're responsible for the security of the equipment once it is delivered to your site. If the equipment is delivered to you before installation, you're responsible for making the equipment available for installation. If equipment isn't available for installation and as a result we need to reschedule installation, there may be a delay and extra cost to you.

Equipment you buy from us

6.3 If you buy equipment from us, you own it once we receive the purchase price. If you cancel your order for the purchase of equipment and we have already ordered the equipment, you may have to pay for the equipment that has been ordered for you. If this happens, you can keep the equipment that you've paid for.

6.4 We procure the right for you to use any software that forms part of the equipment on the same terms that the relevant third party vendor grants such licences. You agree to comply with the licence terms.

6.5 You must ensure that you comply with any reasonable directions that we give you to prepare your site for equipment installation (at your expense). If your site isn't ready for installation and as a result we need to reschedule installation, there may be a delay and extra cost to cover our extra expenses in rescheduling.

6.6 You must obtain our prior written consent before repairing or servicing the equipment.

6.7 You mustn't alter the labels or other identifying marks on any equipment that we provide to you.

6.8 If we provide the Managed Security Service for equipment that you haven't rented or bought from us, you're responsible for any faults with that equipment. We may not be able to meet our obligations if there's a fault with your equipment.

6.9 If we're providing the Managed Security Service for your servers, you may need to install certain software on your servers before we can provide you with the service.

Equipment you rent from us

6.10 If you choose to rent equipment from us, then clauses 6.10 to 6.19 apply to you.

6.11 You don't have any title to any equipment that you rent from us.

6.12 You have to:

(a) keep the rental equipment in good order and repair;

(b) not sell, dispose of or encumber the rental equipment; and

(c) allow us (or our supplier) to inspect the rental equipment at any reasonable time.

6.13 We can charge you additional amounts if you modify the rental equipment without our written consent, and the modifications reduce the equipment's use or value. We only charge you a genuine pre-estimate of our loss.

6.14 If you remove a part of the rental equipment, then you have to replace the removed part at your own cost with a part that's of equal or better quality (**Replacement Part**). The Replacement Part forms part of the rental equipment.

6.15 You can remove any part of the rental equipment that you've added provided that:

(a) it's not a Replacement Part (unless the Replacement Part is being replaced); and

(b) the removal of the Replacement Part doesn't reduce the equipment's use or value.

6.16 We can increase your rental charges if we supply extra parts or upgrades to the rental equipment. We'll tell you if this happens.

6.17 If any item of the rental equipment is lost, stolen or damaged beyond economic repair (except if caused by our breach or negligence), then you have to notify us promptly and pay us the present value of the rental equipment. If this happens before the end of the rental term for the rental equipment, you may also have to pay us early termination charges.

6.18 If you service or maintain the rental equipment, then you have to comply with the vendor's specifications and any other reasonable requirements.

6.19 You have to hold adequate insurance for the full value of the rental equipment and for your ability to pay all rental charges. You have to show us the insurance policy if we ask.

7 EQUIPMENT INSTALLATION

7.1 We install your rental equipment if you ask us to. We charge you an extra amount for this service, and we'll tell you what it is before we commence the installation.

7.2 Our standard hours for installation of equipment are during our standard business hours. If you ask us to install equipment outside our standard business hours we may charge you an additional charge.

7.3 If you don't provide us with access to your site, we can't install the equipment (and we won't be responsible for any installation delays).

7.4 If the installation of your equipment is more complex than we reasonably expect, we may charge an additional amount to cover any additional expense to us. We'll let you know if this is the case.

8 YOUR MANAGED SECURITY SERVICES

8.1 Your application form sets out the details of the Managed Security Services you've chosen.

8.2 We aim to meet the estimated timeframes and delivery dates set out in your application form but can't guarantee to do so. The time estimates in your application form are based on our previous experience, assumptions as to the nature of your internal environment, the availability of our consultants at the time of contract and the timeliness of your inputs and materials. As a result, any indications we give about delivery dates are only estimates and may change.

Changing your Managed Security Services

8.3 You can change any Managed Security Service to a higher-priced version of the same Managed Security Service at any time. The change, including higher charges, will take effect as soon as we process the request. These changes do not affect the term of your Managed Security Service.

8.4 If you try to change you Managed Security Service to a lower-priced version of the same Managed Security Service, this is treated as an early termination under clause13.6.

Your responsibilities

8.5 You have to make sure we have your most current details at all times. You can change your details through the Telstra Security Portal.

8.6 We need you to provide various inputs and do various things in order for us to perform the Managed Security Services. These are different for each service, and are set out in our Responsibilities Guide. We make the Responsibilities Guide available at https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/business-a-full/managedsecurity-responsibilities.pdf

8.7 The Responsibilities Guide may change over time and it's up to you to make sure you have the latest version.

8.8 If your particular environment involves special requirements or extra inputs from you, then these are set out in your application form. These are on top of your responsibilities set out in the Responsibilities Guide or Our Customer Terms.

8.9 You have to provide all materials and inputs by the dates specified in your application form or, where no dates are specified, when we tell you.

8.10 You have to maintain the firmware and software on your equipment (whether you own it or buy or rent it from us) to a currency of no less than 2 versions behind the latest production release of the relevant firmware or software (i.e. n-2).

8.11 We aren't responsible for any delay or increase in cost as a result of you not doing anything you have to do. It may also mean that we can't provide your chosen Services at all.

9 WARRANTIES AND LIABILITY

9.1 We don't offer a voluntary warranty against defects for equipment, but we use reasonable endeavours to pass on the benefit of any manufacturer's warranties applicable to the equipment. The Australian Consumer Law may also provide rights in relation to equipment you buy from us.

9.2 If the equipment is faulty during the term, you must call our telephone service desk to let us know.

9.3 Except where otherwise provided by law, you're responsible for the costs associated with claiming under this clause.

9.4 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we aim to, but can't guarantee, that the Managed Security Services will produce particular results or outcomes for you (such as achieving external certification, accreditation or industry standards). In particular, internet policies and security can't detect every possible limitation or fraudulent activity, and subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we can't guarantee that your systems will operate in an error-free way, or that they'll be safe from malicious attack.

9.5 You have to assess whether any of our recommendations are appropriate for you before you implement them or ask us to implement them for you.

Risks and permissions

9.6 You acknowledge that:

(a) subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, the Managed Security Services may result in interruptions, loss and damage to you, including to your computer systems, networks, websites, software, hardware, internet connections and data;

(b) subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, security testing is inherently risky and carried out over public networks, which may result in unexpected outcomes like system crashes or the inadvertent disclosure of information;

(c) as part of the Managed Security Services, we actively attempt to breach security controls and gain access to your systems, which may be criminal activity if we did it without your permission, so you are giving us that permission throughout the term of the Managed Security Services;

(d) if any of our activities are reported to an external body or authority, you'll do everything necessary to make sure that body is aware you authorised the activities involved in the Managed Security Services; and

(e) our services are based on information you give us and the infrastructure you have in place at the time we perform the Managed Security Services.

10 INTELLECTUAL PROPERTY RIGHTS

10.1 We own all intellectual property rights in any material we develop for you in carrying out the Managed Security Services (including in any reports or materials generated or provided to you as part of your Vulnerability Management service).

10.2 Where we have designed your service we own all intellectual property rights connected with the design, including in the network diagrams, management IP addresses and equipment configurations (**Items**).

10.3 We grant you a licence to use the Items solely for the purpose of your service. The licence ends on expiry or termination of your relevant service.

10.4 The network diagrams and other information that we supply you with your service is confidential information to us. You must ensure that you keep the network diagrams and

other information confidential. You may only disclose the network diagrams and other information in your business for the purposes of using your service (unless you have our prior written consent to do otherwise).

11 CHARGES

11.1 The charges for the service are set out in your application form. All charges are exclusive of GST.

11.2 We'll tell you the pricing for optional services when you request them.

11.3 You have to pay us the charges at the times set out in your application form, or if no time is set out, then before we start providing the service.

Annual CPI Adjustment

11.4 This clause applies if you sign up to or recontract your Managed Security Service on or after 21 February 2024 and the service has a minimum term of 12 months or longer:

(a) The prices for the service will remain fixed during the first 12 months from the commencement of the minimum term (**Start Date**).

(b) At any time after the first 12 months, we may, by giving you reasonable advance notice, increase the prices for the service by a percentage amount no greater than CPI (rounded to the nearest dollar), provided that we only exercise this price increase right no more than once in any 12-month period.

(c) In this clause, **CPI** means the percentage annual change in the Consumer Price Index All Groups weighted average for the 8 capital cities as published by the Australian Bureau of Statistics (ABS) immediately before the date of our price increase notice.

12 TELSTRA SECURITY PORTAL

12.1 We provide you with access to the Telstra Security Portal so you can use the services.

12.2 Your use of the Telstra Security Portal is subject to any separate terms of use that apply to it from time to time.

13 TERM AND TERMINATION

13.1 We provide your Managed Security Services for the period you nominate in your application form, unless terminated earlier in accordance with this clause.

13.2 The minimum term for each component of your Managed Security Service is 12 months (or the longer period set out in your application form).

13.3 The minimum term:

(a) is separate for each Managed Security Service; and

(b) must be the same as the period you have rented equipment from us (if applicable).

13.4 After the minimum term:

(a) your Managed Security Service continues until terminated; and

(b) either you or we may terminate your Managed Security Service in whole or in part by giving at least 30 days written notice.

13.5 Where you rent equipment from us after the minimum term, you may:

(a) keep renting the equipment from us;

(b) give the equipment back to us; or

(c) if we agree, buy it from us (we'll tell you the price when you ask us).

13.6 If you or we terminate your Managed Security Service during the minimum term for any reason other than our material breach or our inability to support your equipment (except where we can't support your equipment because you haven't maintained the firmware or software to the required currency, in which case this clause does apply), you have to:

(a) pay us the early termination charges for that Managed Security Service; and

(b) pay the full amount of all rental payments that you'd have made during the term of your rental agreement with us for that equipment. In exchange for making those payments, we'll give you title in the equipment.

13.7 The early termination charges for the Managed Security Service and Internet Protection Services are equal to the actual costs and expenses that we have incurred or committed to in anticipation of providing the service to you and that cannot be reasonably avoided by us as a result of the cancellation, which will not exceed an amount calculated as follows:

For Cyber Detection and Preseason-Endpoint and Internet Protection Services:

ETC = (A x B) x 80%

For other Managed Security Services:

ETC = (A x B) x 50%

where:

A = number of months remaining in minimum term for the terminated service (as set out in your application form)

B = the monthly charge for the terminated service (as set out in your application form)

13.8 You acknowledge the early termination charges are a genuine pre-estimate of the loss we'd suffer if you terminated early.

13.9 We can terminate any or all of your Managed Security Services if you cause a defect or incident by accidental damage, or improper or negligent use of the equipment or the network, or you don't maintain the currency of the firmware or software on your equipment as required by clause 8.10. You have to pay early termination charges if we terminate your Managed Security Service under this clause.

13.10 We can terminate your Managed Security Service in respect of a particular device in accordance with the General Terms of Our Customer Terms.

13.11 If you rent a device from us, we can suspend or cancel your service in accordance with the General Terms of our Customer Terms.

14 SPECIAL MEANINGS

14.1 The following words have the following special meanings:

Incident means a Security Event that we consider poses a real risk to your systems or environment.

Responsibilities Guide means the guide we publish that sets out your responsibilities regarding the Managed Security Services, as updated from time to time.

Security Event means an observable change to the normal behaviour of your system, environment, process, workflow or person occurrence that may pose a security risk to your systems or environment.

Priority 1 Incident means an Incident where your service is not available at a site (or multiple sites) causing critical impact to business operations.

Priority 2 Incident means an Incident where your service is not available, or severely degraded, impacting significant aspects of business operations.

Priority 3 Incident means an Incident where your service is degraded. Customer service is noticeably impaired, but most business operations continue.

Priority 4 Incident means all other Incidents that are not Priority 1, 2 or 3 Incidents.