Service Terms

Cyber Detection and Response Section

1 ABOUT THIS DOCUMENT

1.1 Where this document fits into our agreement with you

a) This is the Cyber Detection and Response section of Our Customer Terms.

b) Unless you have a separate agreement with us which excludes them, the **General Terms of Our Customer Terms** apply to the provision of Cyber Detection and Response services.

c) Certain words are used with the specific meanings set out in this section or in the General Terms of Our Customer Terms.

1.2 Inconsistencies

a) If the General Terms of Our Customer Terms are inconsistent with something in this section, then this section applies instead of the General Terms to the extent of the inconsistency.

b) 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 of Our Customer Terms.

PART A: Cyber Detection and Response Enterprise

2 SERVICE SUMMARY

2.1 What is Cyber Detection and Response Enterprise?

a) Cyber Detection and Response (**CDR**) Enterprise is a managed cyber security detection and response service.

b) CDR Enterprise comprises the following core operational capabilities:

   i. logging – this service stores the log and event data we receive from your Data Sources;

   ii. event monitoring, correlation and classification – this service monitors logs and events for Incidents;

   iii. incident notification – this service provides notification to you of Incidents and may include a priority rating of these Incidents; and

   iv. managed detection and response – this service provides responses to Incidents based on your selected risk profile(s).

c) You may also select Vulnerability Scanning – this service scans for vulnerabilities in the Assets that we've agreed with you.

d) We provide the CDR Enterprise service using shared infrastructure and the public cloud, unless we otherwise think it's appropriate to use dedicated infrastructure.

2.2 Eligibility

a) The CDR Enterprise services are not available to Telstra wholesale customers or for resale.

b) To provide the CDR Enterprise services, we need to be able to connect to your Data Sources. We'll tell you when you apply for the CDR Enterprise services what the minimum connectivity requirements are.

c) There are elements of the CDR Enterprise 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.

d) To receive the CDR Enterprise service, you must at your own cost:

   i. separately obtain an appropriate carriage service;

   ii. ensure the term of that carriage service does not end before the term of your CDR Enterprise service; and

   iii. 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.

2.3 Your responsibilities

a) You must make sure we have your most current details at all times. For CDR Enterprise you can change your details through the Telstra Security Portal.

b) If your environment involves special requirements or extra inputs from you, then these are set out in your Service Order Form. These are on top of your responsibilities set out in this section of Our Customer Terms.

c) You must provide all materials and inputs by the dates specified in your Service Order Form or, where no dates are specified, when we tell you.

d) You must maintain the firmware and software on your equipment (whether you own it or buy, lease 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).

e) 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 CDR Enterprise services at all.

2.4 Fair Usage Policy

a) Data ingested into the CDR Enterprise platform from your Data Sources must only be for legitimate business purposes and align with the scope and nature of the CDR Enterprise service.

b) We reserve the right to monitor data ingestion levels and patterns to ensure the intended functionality of the CDR Enterprise service and compliance with this policy.

c) If there are material and sustained variations, you must cooperate with us to identify the cause and bring the ingestions levels back within the expected parameters.

d) If it is not possible to bring the ingestion levels back within the expected parameters, we reserve the right to move you to non-standard pricing. If you do not accept the revised price, you may cancel your CDR Enterprise service.

2.5 Warranties and Liability

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

b) Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we aim to, but can't guarantee, that the CDR Enterprise services will produce particular results or outcomes for you (such as achieving external certification, accreditation or meeting 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, viruses and other unauthorised access to your network.

c) You must assess whether any of our recommendations are appropriate for you before you implement them or ask us to implement them for you.

d) You acknowledge that:

   i. subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, the CDR Enterprise services may result in interruptions, loss and damage to you, including to your computer systems, networks, websites, software, hardware, internet connections and data;

ii. 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 CDR Enterprise services; and

iii. our services are based on information you give us and the infrastructure you have in place at the time we perform the CDR Enterprise services.

2.6 Intellectual Property Rights

a) We own all intellectual property rights in any material we develop for you in carrying out the CDR Enterprise services (including in any reports or materials generated or provided to you as part of your Vulnerability Scanning service).

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

c) 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 CDR Enterprise service.

d) The Items that we supply you with your CDR Enterprise service is confidential information to us. You must ensure that you keep the Items confidential. You may only disclose the Items in your business for the purposes of using your CDR Enterprise service (unless you have our prior written consent to do otherwise).

2.7 Service term

a) We provide CDR Enterprise for the period you nominate in your Service Order Form, unless terminated earlier in accordance with this clause.

b) The minimum term for each component of CDR Enterprise is 12 months (or the longer period set out in your Service Order Form).

c) After the minimum term:

i. your CDR Enterprise service continues until terminated; and

ii. either you or we may terminate your CDR Enterprise service in whole or in part by giving at least 30 days written notice.

2.8 Cancellation

a) We can terminate your CDR Enterprise service if you cause a defect or incident by accidental damage, or improper or negligent use of the service, or you don't maintain the currency of the firmware or software on your equipment. You have to pay early termination charges if we terminate your CDR Enterprise service under this clause.

b) When you cancel your CDR Enterprise service:

i. we will store your logs up to the date of cancellation (at your expense), unless you tell us in writing that you request for us to retain these logs for a further period and that you agree to the charges for such storage (Further Storage Period);

ii. you may request an extract of your logs before you cancel or during the Further Storage Period;

iii. you must pay a fee for this extraction and we can confirm this fee on request;

iv. you will not be able to request an extract after the Further Storage Period; and

v. your Vulnerability Scanning service will also be cancelled and we won't retain any scan data or reports.

2.9 Early Termination Charges

a) If you or we terminate your CDR Enterprise 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 version, in which case this clause does apply), we may require you to reimburse us for:

i. any charges incurred up to the date of termination;

ii. any discounts we applied to the relevant services from the commencement of billing until the termination date; and

iii. if you have Vulnerability Scanning, 100% of any third-party licence costs for the remaining 12-month period.

ⓘ For example if you cancel 3 months into a 36-month term we may charge you 9 months licence fees or if you cancel 13 months into a 36 month term we may charge you 11 months licence fees.

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

3 CHARGES

3.1 Standard Charges

Where to find your charges

a) The charges for your CDR Enterprise service are set out in your Service Order Form.

b) We'll tell you the pricing for optional and non-standard services when you request them.

When monthly billing starts

a) You have to pay us the charges at the times set out in your Service Order Form, or if no time is set out, then from the date we have onboarded your first nominated Data Source and we start providing the CDR Enterprise service.

How are prices calculated

a) We charge for the CDR Enterprise service on a per Endpoint basis. We will agree the initial number of Endpoints with you, and this will be set out in the Service Order Form. The number of Endpoints will determine the applicable pricing tier. The minimum number of Endpoints is 100.

b) We will periodically ask you to validate the number of Endpoints. If the number of Endpoints has changed, we will apply the applicable pricing tier for the updated number of Endpoints.

3.2 Annual CPI Adjustment

a) This clause applies if your CDR Enterprise service has a minimum term of 12 months or longer:

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

ii. 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.

iii. 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.

4 INCLUSIONS

4.1 Standard inclusions

a) All of the Core Operational Capabilities are included as standard. If you ask for us to only provide some but not all of the Core Operational Capabilities, we may be able to offer a customised solution but on non-standard pricing.

b) The following types of Data Sources are included as standard:

i. Identity,
ii. Cloud Access Security Broker,
iii. Cloud,
iv. DNS,
v. DHCP,
vi. Endpoint Detection & Response,
vii. Email Proxy,
viii. Firewall,
ix. Hypervisor,
x. OS,
xi. SD-WAN,
xii. VPN and
xiii. Web Proxy.

c) All standard Data Sources types are agreed with us during the pre-sales process. No additional fees will apply for any parser or detection development required to activate the agreed Data Sources. During the pre-sales process, if you request a non-standard Data Source we may be able to offer a customised development option for an additional charge.

d) You can add, remove or change your Data Sources at any time. Provided they are listed as standard, and it does not cause a breach the Fair Use Policy there will be no impact to your charges.

e) If you send us logs from non-standard Data Sources or a change to your Data Sources causes a breach of the Fair Use Policy, then we reserve the right to move you to non-standard pricing. If you do not accept the revised price, you may cancel your CDR Enterprise service.

f) Monitoring of your corporate network is included. Additional charges will apply if you ask us to monitor ancillary networks.

4.2 Service Stages

a) Activation of the CDR Enterprise service comprises one or more milestones and deliverables. Stage 3 Data Source onboarding can only commence from when we receive and validate your Log Events.

b) Provisioning of the Vulnerability Scanning service depends on separate inputs being completed before the service is live that are detailed in clause 5.1b).

	Stage 1 Kick-off	Stage 2 Business Onboarding	Stage 3 Data Source Onboarding	Stage 4 Security Monitoring
Our Inputs	▪ Validate the scoped Data Sources.	▪ Build the log collector(s). ▪ Configure the portal tenant and users. ▪ Enable cold storage. ▪ Create the ticketing queue. ▪ Configure Data Sources that use a pull mechanism to ingest logs into the Cyber Detection and Response platform.	▪ Validate logs for security outcomes. ▪ Complete device mappings ▪ Create or apply security use cases. ▪ Develop or apply parsers. ▪ Create or apply detections. ▪ Release parsers.	▪ Live security monitoring achieved. ▪ Provision access to the Telstra Security Portal ▪ Conduct customer welcome session and Telstra Security Portal training. ▪ Commence billing. ▪ Setting up monthly customer security partnership meeting ▪ Detection maturation and tuning ▪ Implementation and deployment of XSOAR capability and pre-approved response actions agreed between the TSOC and customer. ▪ Setup and activation of Qualys scanner if the Vulnerability Scanning add-on has been purchased. ▪ Activation of Managed Extended Detection and Response capability and agreed pre response actions
Your inputs		▪ Populate the Customer Information Form. ▪ Deploy the log collector(s). ▪ Implement designated firewall rules. ▪ Configure Data Sources that use a push mechanism to forward logs to the log collector(s). ▪ Share credentials for Data Sources that use a pull mechanism for log forwarding. ▪ Provide access to supported Endpoint Detection Response tool.	▪ Provide inputs to security use case development and tuning as required.	
Shared inputs	▪ Provide end-to-end onboarding process and	▪ Schedule and conduct regular meetings.		

	log collector installation overview. ▪ Conduct a joint kick-off session.	▪ Complete IP whitelisting.		

4.3 Managed Detection and Response Actions

a) We will take the response actions outlined the table below based on the profile(s) you have selected.

	Profile		
Response Actions	**Cautious**	**Measured**	**Active**
Automated Response			
Quarantine File	Yes	Yes	Yes
Upload File for Analysis	Yes	Yes	Yes
Event Log Review	Yes	Yes	Yes
Manual Response			
End process, Stop Service, or Disable Registry	No	Yes	Yes
Isolate System	No	No	Yes
Restart System	No	No	Yes

4.4 Retention Periods

a) We archive all log data for 2 years. Longer period of retention may be available for an additional cost.
b) You can access and search the previous 14 days of log data via OpenSearch.

4.5 Accessing your CDR Enterprise service

a) You can access your CDR Enterprise service via the Telstra Security Portal.
b) The Telstra Security Portal aims to let you do the following:
   i. Acquire insight into active Incidents, Log Event, Alert and Incident trends.
   ii. View and track prioritised Incidents with expert assessment.
   iii. View and track service requests
   iv. Acquire insight into service operational performance
   v. Configure and run vulnerability scans, view vulnerabilities by severity against assets, run and download reports

4.6 Service Limitations

a) Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we don't promise that the CDR – Enterprise service will correctly detect and identify all:
   i. Security Events or Incidents;
   ii. unauthorised access to your network;
   iii. viruses;
   iv. spam; or
   v. other types of attacks or issues.
b) You must promptly tell us if you find limitations or issues with your CDR – Enterprise service.
c) 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 Scanning service).

5 ADD-ONS

5.1 Vulnerability Scanning

a) The Vulnerability Scanning is an optional service that:
   i. remotely scans IT assets and IP addresses that we've agreed with you, against a list of known security vulnerabilities; and
   ii. is self-service so you can schedule scans, view configurations, and run and download reports via the Telstra Security Portal.

b) To obtain the Vulnerability Scanning service, if we ask you to, you must promptly and at your own cost:
   i. decide which IP ranges are to be scanned and the number of internal virtual appliances required;
   ii. deploy internal scanning appliances;
   iii. configure your systems to allow your assets to be scanned (such as implementation of firewall rule changes);
   iv. conduct asset discovery (map) scans;
   v. classify assets. (Critical/Non Critical or other);
   vi. set up scans schedules and reporting schedules; and
   vii. comply with our other reasonable requests.

c) You must back up all of your data, whether contained in or available from your assets that will be scanned. We are not liable for any loss or corruption of data, including where this occurs in connection with the Vulnerability Scanning service. 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.

d) You agree that for your Vulnerability Scanning service:
   i. scan reports show a point in time of your assets at the time of the scan;
   ii. your scan uses a list of known vulnerabilities, which is continually updated, and this may impact the currency of your scan reports;
   iii. scans don't detect all vulnerabilities or vulnerabilities that are known at the time of the scan;
   iv. you're responsible for scheduling scans at appropriate intervals based on your security needs; and
   v. the service doesn't test, exploit, manage, rectify or fix any vulnerabilities or issues these are your responsibility.

e) Given the nature of the service, the service levels in this section of Our Customer Terms don't apply to your Vulnerability Scanning service.

f) You must:
   i. only use the Vulnerability Scanning service (and any reports generated) solely for your internal use and to scan assets that you have the legal right to scan;
   ii. not scan the assets of a third party; and
   iii. not modify, interfere with, transfer, or affect the operation of the Vulnerability Scanning service in any way.

g) You may use up to one Virtual Scanner per 100 IP Addresses scoped for the Vulnerability Scanning service up to a maximum up 10 scanners. The minimum number of IP addresses you can use is 100.

5.2 Other work we do

a) You may request:
   i. additional log and event storage capacity;
   ii. services to extract your logs from storage; and
   iii. scanning of additional IP addresses above your applicable tier for your Vulnerability Scanning service.
   iv. provision of additional virtual scanners for your Vulnerability Scanning service.

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

6 SERVICE MANAGEMENT

6.1 Service Provisioning

a) We aim to meet any estimated timeframes and delivery dates set out in your Service Order Form but can't guarantee to do so. Time estimates in your Service Order 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.

b) The activation service level for CDR Enterprise is:

Item	Description	Service Level Target
Data Source onboarding	The time from when we validate receipt of data for each individual Data Source to when we commence live monitoring.	6 weeks

c) Our activation service level assumes the following:

i. the relevant business onboarding inputs detailed in clause 4.2 are complete;

ii. timing begins for each Data Source when data starts being forwarded from your network to the CDR -Enterprise Platform, and we have validated receipt of those data;

iii. timing excludes any time waiting for you to provide information we need to progress your service activation;

iv. timing excludes any time needed to alter or prepare your network, devices, or other resources in connection with the service activation; and

v. the service level target does not apply to types of Data Sources that we have not previously onboarded. These Data Sources take longer to activate whilst the requisite development work is completed. We will provide an estimated onboarding time during the onboarding process upon review of the data source.

6.2 Change Management

a) If you want to:

i. Increase or reduce your scoped Endpoints;

ii. Add or remove a non-standard Data Source;

iii. Add or remove coverage of an ancillary network;

iv. Change your service Core Operational Capability; and

v. Change your log retention period,

we will assess and advise you if the changes are considered standard or non-standard and if it will impact your Endpoint unit price.

b) You can increase the number of IP Addresses scoped for the Vulnerability Scanning add-on at any time.

c) Downgrades to the number of IP Addresses scoped for the Vulnerability Scanning feature may trigger a once off downgrade fee equivalent to the Vulnerability Scanning early termination charge for each IP address removed.

d) All changes, including increased or reduced service fees, will take effect as soon as we process the request and do not affect the minimum term of your CDR Enterprise service.

6.3 Service Quality

a) We aim to meet the following service quality targets:

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	NA
		4	NA
		1	Portal + email + phone call

	Incident notification method	The method we use to notify your nominated contact person of Incidents	2	Portal + email + Phone call
			3	Portal
			4	Portal
	Service management	How often we contact you about your CDR service	NA	Monthly

6.4 Service Availability

a) We aim to meet the following service availability targets:

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	99.9%

b) Availability is calculated using the following formula:

Service 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.

6.5 Fault reporting

a) We aim to meet the following fault reporting targets:

Item	Description	Platform Incident Priority Level	Service level target
Initial response time for faults	Measured from when a fault is reported to when we respond	1	30 mins
		2	60 mins
		3	120 mins
		4	240 mins
Service restoration	Measured from when a fault is reported to when the fault is resolved	1	95% restored (or work around) in 6 hours
		2	95% restored (or work around) in 12 hours
		3	95% restored (or work around) in 24 hours
		4	95% restored (or work around) in 72 hours
Progress updates	Measured from when we last updated you on the issue	1	every 1 hour
		2	every 4 hours

			3	every 12 hours
			4	every 24 hours

6.6 Rating and notification of Incidents

a) As part of your CDR Enterprise 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

b) 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.

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

6.7 Service Level Exclusions

a) We are not responsible for failing to meet the service level targets in this clause 6 where the failure to meet the service level target is affected by:

i. a fault with your product, service or resource that is caused by you or a third party;
ii. any third-party act or omission;
iii. the cutting of cable or fibre which is needed to provide your product or service;
iv. interference or damage to our equipment or network by you or by a third party;
v. a fault beyond our CDR Enterprise platform or with your Assets or Data Sources (unless we have specifically agreed in writing to support these things); or
vi. 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).

6.8 Missed service level targets

a) If we do not meet the service level targets in this clause 6 in two consecutive months, then you may cancel your CDR service and we will waive any applicable early termination charges.

7 DICTIONARY

7.1 Dictionary

a) **Asset** means 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.

b) **Core Operational Capability** means the capabilities listed in clause a)b).

c) **Data Sources** means the network components you have selected to send logs to us.

d) **Endpoints** means the devices connected to your network such as desktop and laptop computers, servers, virtual machines, mobile devices and Internet of Things (IOT) devices.

e) **Impact** means how severe we think the Incident is on an Asset.

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

g) **Items** has the meaning given in clause b).

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

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

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

k) **Priority Incident** means all other Incidents that are not Severity 1, 2 or 3 Incidents.

l) **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.

m) **TSOC** or **Telstra Security Operations Centre** means Telstra's security operations centre.

n) **Urgency** means how soon we think the Incident needs to be addressed.

PART B: Cyber Detection and Response Sentinel

8 SERVICE SUMMARY

8.1 What is Cyber Detection and Response Sentinel?

a) Cyber Detection and Response (**CDR**) Sentinel is a managed cyber security detection and response service.

b) CDR Sentinel monitors your Data Sources connected to your instance of Microsoft Sentinel and comprises the following core operational capabilities:

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

(ii) incident notification this service provides notification to you of Incidents and may include a priority rating of these Incidents.

c) We provide the CDR Sentinel service using Microsoft 365 Lighthouse.

8.2 Eligibility

a) The CDR Sentinel services are not available to Telstra wholesale customers or for resale.

b) To provide the CDR Sentinel services, we need to be able to connect to your instance of Microsoft Sentinel. We'll tell you when you apply for the CDR Sentinel services what the minimum connectivity requirements are.

c) Provisioning of the CDR Sentinel service and onboarding of your Data Sources to your Microsoft Sentinel instance requires a separate professional services engagement with Telstra Purple.

d) There are elements of the CDR Sentinel 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.

e) To receive the CDR Sentinel service, you must at your own cost:

(i) separately obtain an appropriate carriage service;

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

(iii) 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 instance of Microsoft Sentinel to our infrastructure using a means that we require.

f) For us to be able to monitor your environment through Microsoft Sentinel, you must have:

(i) a Microsoft subscription and tenant that includes Microsoft Sentinel, or an individual account with a valid payment method, these are required to access Azure and deploy resources;

(ii) an Azure subscription to track resource creation and billing;

(iii) a Log Analytics workspace is required to house the data that Microsoft Sentinel ingests and analyses for detections, analytics, and other features; and

(iv) any other Pre-requisites as required by Microsoft.

g) You must provide our personnel with appropriate access levels to your Azure tenancy and Sentinel instance to ensure we can effectively onboard, configure, monitor, manage, and respond to security events.

8.3 Your responsibilities

a) You must make sure we have your most current details at all times.

b) If your environment involves special requirements or extra inputs from you, then these are set out in your Service Order Form. These are on top of your responsibilities set out in this section of Our Customer Terms.

c) You must provide all materials and inputs by the dates specified in your Service Order Form or, where no dates are specified, when we tell you.

d) You must maintain the firmware and software on your equipment (whether you own it or buy, lease 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).

e) 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 CDR Sentinel services at all.

8.4 Fair Usage Policy

a) Data ingested into the CDR Sentinel platform from your Data Sources must only be for legitimate business purposes and align with the scope and nature of the CDR Sentinel service.

b) We reserve the right to monitor data ingestion levels and patterns to ensure the intended functionality of the CDR Sentinel service and compliance with this policy.

c) If there are material and sustained variations, you must cooperate with us to identify the cause and bring the ingestions levels back within the expected parameters.

d) If it is not possible to bring the ingestion levels back within the expected parameters, we reserve the right to move you to non-standard pricing. If you do not accept the revised price, you may cancel your CDR Sentinel service.

8.5 Warranties and Liability

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

b) Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we aim to, but can't guarantee, that the CDR Sentinel services will produce particular results or outcomes for you (such as achieving external certification, accreditation or meeting 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, viruses and other unauthorised access to your network.

c) You must assess whether any of our recommendations are appropriate for you before you implement them or ask us to implement them for you.

d) You acknowledge that:

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

(ii) 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 CDR Sentinel services; and

(iii) our services are based on information you give us and the infrastructure you have in place at the time we perform the CDR Sentinel services.

8.6 Intellectual Property Rights

a) We own all intellectual property rights in any material we develop for you in carrying out the CDR services.

b) 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**).

c) 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 CDR Sentinel service.

d) The Items that we supply you with your CDR Sentinel service is confidential information to us. You must ensure that you keep the Items confidential. You may only disclose the Items in your business for the purposes of using your CDR Sentinel service (unless you have our prior written consent to do otherwise).

8.7 Service term

a) We provide CDR Sentinel for the period you nominate in your Service Order Form, unless terminated earlier in accordance with this clause.

b) The minimum term for each component of CDR Sentinel is 12 months (or the longer period set out in your Service Order Form).

c) After the minimum term:

(i) your CDR Sentinel service continues until terminated; and

(ii) either you or we may terminate your CDR service in whole or in part by giving at least 30 days written notice.

8.8 Cancellation

a) We can terminate your CDR Sentinel service if you cause a defect or incident by accidental damage, or improper or negligent use of the service, or you don't maintain the currency of the firmware or software on your equipment. You have to pay early termination charges if we terminate your CDR Sentinel service under this clause.

8.9	**Early Termination Charges**
	a) If you or we terminate your CDR Sentinel 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),we may require you to reimburse us for: (i) any charges incurred up to the date of termination; (ii) any discounts we applied to the relevant services from the commencement of billing until the termination date. b) You acknowledge the early termination charges are a genuine pre-estimate of the loss we'd suffer if you terminated early.

9 CHARGES

9.1	**Standard Charges**
Where to find your charges	a) The charges for your CDR Sentinel service are set out in your Service Order Form. b) We'll tell you the pricing for optional and non-standard services when you request them. c) The following costs are separate from and in addition to the CDR Sentinel charges: (i) the professional services engagement for onboarding and configuration; and (ii) costs associated with eligibility requirements in clause 2.2(e).
When monthly billing starts	d) You have to pay us the charges at the times set out in your Service Order Form, or if no time is set out, then from the date when ongoing monitoring commences and we start providing the CDR Sentinel service.
How are prices calculated	e) We charge for the CDR Sentinel service on a per Endpoint basis. We will agree the initial number of Endpoints with you, and this will be set out in the Service Order Form. The number of Endpoints will determine the applicable pricing tier. The minimum number of Endpoints is 100. f) We will periodically ask you to validate the number of Endpoints. If the number of Endpoints has changed, we will apply the applicable pricing tier for the updated number of Endpoints.
9.2	**Annual CPI Adjustment**
	a) This clause applies if your CDR Sentinel service has a minimum term of 12 months or longer: (i) The prices for the service will remain fixed during the first 12 months from the commencement of the minimum term (Start Date). (ii) 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. (iii) 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.

10 INCLUSIONS:

10.1	**Standard Inclusions**
	a) All of the Core Operational Capabilities are included as standard. If you ask for us to only provide some but not all of these Core Operational Capabilities, we may be able to offer a customised solution but on non-standard pricing. b) The following types of Data Sources are included as standard: (i) Identity, (ii) Cloud Access Security Broker, (iii) Cloud, (iv) DNS, (v) DHCP, (vi) Endpoint Detection & Response, (vii) Email Proxy,

(viii) Firewall,
(ix) Hypervisor,
(x) OS,
(xi) SD-WAN,
(xii) VPN and
(xiii) Web Proxy.

c) All standard Data Sources types are agreed with us during the pre-sales process. No additional fees will apply for any detection development required to activate the agreed Data Sources. During the pre-sales process, if you request a non-standard Data Source we may be able to offer a customised development option for an additional charge.

d) You can add, remove or change your Data Sources at any time. Provided they are listed as standard, and it does not cause a breach the Fair Use Policy there will be no impact to your charges.

e) If you send us logs from non-standard Data Sources or a change to your Data Sources causes a breach of the Fair Use Policy, then we reserve the right to move you to non-standard pricing. If you do not accept the revised price, you may cancel your CDR Sentinel service

f) Monitoring of your corporate network is included. Additional charges will apply if you ask us to monitor ancillary networks.

10.2 Service Stages

a) Activation of the CDR Sentinel service comprises one or more of the following milestones and deliverables.

	Stage 1 **Kickoff**	**Stage 2** **Onboarding Readiness**	**Stage 3** **Monitoring Kickoff**	**Stage 4** **Security Monitoring**
Our inputs	• Telstra Purple Engagement enables Sentinel monitoring by the TSOC team. • During the build stage, TSOC and Purple teams will work together on the items required for monitoring readiness. • Key inputs required are: ORC Checklist + SoW	• Handover from initial Onboarding team to Ongoing Monitoring Team (Purple -> TSOC Ops Team)	• TSOC Team starts monitoring of Sentinel Data Sources, necessary playbooks are set up. • Customer points of contact are identified and notified.	• Live security monitoring achieved • The TSOC team can monitor the CDR Sentinel instance via an established mechanism. • The customer can receive incidents and alert notifications via agreed methods and contact details. • Commence billing • Setting up monthly customer security partnership meeting
Your inputs	• Access to necessary environments and details for Telstra teams	• Support to the required personnel with access and other environment details.	• Customer personnel who can support levels of escalation. • Provide inputs to security use case development and tuning as required	• Monthly Check-in meeting participation • Providing information about the number of endpoints and supporting ongoing tuning of Sentinel playbooks •

10.3 Accessing your CDR Sentinel service

a) You can access a dashboard in Microsoft Sentinel that will show operational and health insights.

10.4 Service Limitations

a) Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we don't promise that the CDR Sentinel service will correctly detect and identify all:
   (i) Security Events or Incidents;
   (ii) unauthorised access to your network;
   (iii) viruses;
   (iv) spam; or
   (v) other types of attacks or issues.

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

c) You must give us at least 10 business days' notice before any vulnerability or penetration testing occurs to your network.

11 SERVICE MANAGEMENT

11.1 Change Management

a) If you want to:
   (i) Increase or reduce your scoped Endpoints.
   (ii) Add or remove a non-standard Data Source.
   (iii) Add or remove coverage of an ancillary network.
   (iv) Change your service Core Operational Capability.
   (v) Change your log retention period,

   we will assess and advise you if the changes are considered standard or non-standard and if it will impact your Endpoint unit price.

b) All changes, including increased or reduced service fees, will take effect as soon as we process the request and do not affect the minimum term of your CDR Sentinel service.

11.2 Service Quality

a) We aim to meet the following service quality targets:

Item	Description	Incident Priority	Service level target
Incident rating time	Time from when Microsoft Sentinel receives a Security Event to the time an Incident is rated	1	15 mins
		2	30 mins
		3	60 mins
		4	180 mins
Incident notification time	Time from when the Microsoft Sentinel platform notifies the Telstra SOC analyst of an alert, to 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	email + phone call
		2	email
		3	Customer Sentinel Dashboard
		4	Customer Sentinel Dashboard

	Service management	How often we contact you about your CDR Sentinel service	NA	Monthly

11.3 Fault reporting

a) We aim to meet the following fault reporting targets:

Item	Description	Platform Incident Priority	Service level target
Initial response time for faults	Measured from when a fault is reported to when we respond	1	30 mins
		2	60 mins
		3	120 mins
		4	240 mins
Service restoration	Measured from when a fault is reported to when the fault is resolved	1	95% restored (or work around) in 6 hours
		2	95% restored (or work around) in 12 hours
		3	95% restored (or work around) in 24 hours
		4	95% restored (or work around) in 72 hours
Progress updates	Measured from when we last updated you on the issue	1	every 1 hour
		2	every 4 hours
		3	every 12 hours
		4	every 24 hours

11.4 Rating and notification of Incidents

a) As part of your CDR Sentinel 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

b) 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.

c) You can choose not to receive email or SMS alerts by changing your preferences by contacting your Telstra Customer Enablement contact during the monthly check-in. .

11.5 Service Level Exclusions

a) We are not responsible for failing to meet the service level targets in this clause 11 where the failure to meet the service level target is affected by:

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

(ii) any third-party act or omission;

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

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

(v) a fault with Microsoft Sentinel or with your Assets or Data Sources; or

(vi) 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).

11.6 Missed service level targets

a) If we do not meet the service level targets in this clause 6 in two consecutive months, then you may cancel your CDR service and we will waive any applicable early termination charges.

12 DICTIONARY

12.1 Dictionary

a) **Asset** means 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.

b) **Core Operational Capability** means the capabilities listed in clause 8.1b).

c) **Data Sources** means the network components you have selected to send logs **to us.**

d) **Endpoints** means the devices connected to your network such as desktop and laptop computers, servers, virtual machines, mobile devices and Internet of Things (IOT) devices.

e) **Impact** means how severe we think the Incident is on an Asset.

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

g) **Items** has the meaning given in clause 8.6b).

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

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

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

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

l) **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.

m) **TSOC** or **Telstra Security Operations Centre** means Telstra's security operations centre.

n) **Urgency** means how soon we think the Incident needs to be addressed.