

## OneStream VPN Service Schedule



March 2007

Prepared by: Product Management

1.	DEFINITIONS.....	3
2.	COMMANDER VPN DESCRIPTION .....	4
3.	OneStream VPN COMPONENTS.....	5
4.	SERVICE LEVELS .....	10
5.	ADDS, MOVES & CHANGES .....	13
6.	PROVISIONING .....	14
7.	FAULT REPORTING.....	14
8.	REBATES.....	15
9.	FAULT DETECTION & MANAGEMENT PROCESS .....	16
10.	CONTACT DETAILS .....	17

	<i>Table 1 – Fault Severity Levels .....</i>	<i>3</i>
	<i>Table 2 – OneStream VPN Service Components .....</i>	<i>5</i>
	<i>Table 3 – Core Network Performance Measure .....</i>	<i>6</i>
	<i>Table 4 – Traffic Contract Details.....</i>	<i>7</i>
	<i>Table 5 – QoS Profile Provisioning .....</i>	<i>7</i>
	<i>Table 6 – Current Default Traffic Classification &amp; Marking Configurations .....</i>	<i>9</i>
	<i>Table 7 – Availability Service Level Details.....</i>	<i>10</i>
	<i>Table 8 – Management Service Level Details.....</i>	<i>11</i>
	<i>Table 9 – Supported Adds, Moves and Changes.....</i>	<i>13</i>
	<i>Table 10 – Target Provisioning, Relocation, Adds and Changes Lead Times .....</i>	<i>14</i>
	<i>Table 11 – Fault Classifications .....</i>	<i>14</i>
	<i>Table 12 – Access Type Rebates .....</i>	<i>15</i>
	<i>Table 13 – Notification Schedule.....</i>	<i>16</i>

This Service Schedule forms an integral part of Commander's Standard Form Of Agreement (SFOA) between us and cannot be used as a stand alone agreement. Any terms defined in the Standard Form Of Agreement have the same meaning in this Service Schedule.

This document provides details of the OneStream VPN Service to assist you ("Customer") with an understanding of how the Service Levels are structured, delivered and supported.

## 1. DEFINITIONS

This Service Schedule uses the terms of reference described below.

### 1.1. General Helpdesk Hours

These are the hours in which we are able to accept your call for general and billing enquiries.

### 1.2. Technical Helpdesk Hours

These are the hours in which we are able to accept your call for technical support enquiries and to log a fault with your service.

### 1.3. Provisioning Helpdesk Hours

These are the hours in which we are able to accept your call for provisioning enquiries.

### 1.4. Telephone Response Time

Telephone Response Times relate to the time taken to answer your call at any of our helpdesks whether you are raising a fault, checking your bill or have a general enquiry about your service.

### 1.5. Fault Response Time

Fault Response Time is the time taken by us to call the person nominated by you once a fault has been reported by you or detected by us.

### 1.6. Fault Coverage Hours

Fault Coverage Hours are the hours in which we will work to resolve a fault with your service. Fault Coverage Hours are used in the calculation of availability and rebates for your service.

### 1.7. Fault Severity Levels

Faults are categorised into one of four Severity Levels:

Severity Level	Example fault
1	Customer network, tail or CPE unavailable affecting individual or multiple sites/locations.
2	CPE or network performance impaired whilst most business operations remain functional.
3	Intermittent loss or degradation of service (resolved as no fault found by us).
4	Configuration change or feature enhancement required.

*Table 1 – Fault Severity Levels*

### 1.8. Target Availability

Target Availability is the expected performance for each component of the service.

### 1.9. Unavailable Hours

Unavailable Hours is the total number of hours within a month that a fault of severity level 1 or 2 remains unresolved. Unavailable Hours are measured over the Fault Coverage Hours. Unavailable Hours are calculated from the time when the fault is logged at our Technical Support Desk until your nominated contact is notified that the fault has been rectified.

Unavailable Hours exclude any Scheduled Outages and all faults of severity level 3 or 4. Faults reported to us as severity level 1 or 2, but determined by us not to be a fault with your service, are also excluded.

In addition, any aspect of the service that you have control over, and that affects the service we provide you, is excluded from our calculations.

Unavailable Hours are used in calculating your service availability and rebates.

## **1.10. Planned Outage**

A predefined, routinely scheduled event in which part of the Commander network may be interrupted for the purpose of maintenance or upgrades.

## **1.11. Fault Detection Method**

There are 2 types of fault detection method as described below:

### **1.11.1. Proactive**

Services that are proactively fault managed include the capability for Commander to automatically detect a fault and begin working on the fault before you call us to report the fault. We will call your nominated contact when we detect a fault of severity level 1 to determine whether the fault is valid. All other faults (severity level 2, 3 or 4) should be reported by you at our Technical Helpdesk to ensure we are working on a valid fault. If the fault is not reported at our Technical Helpdesk it will be excluded from our rebate calculations.

### **1.11.2. Reactive**

Services that are reactive are not necessarily monitored and rely on you to report a fault to us.

## **1.12. Time To Detect**

Time To Detect is the time period from when a fault has been detected by our monitoring system until we log it on our fault ticketing system.

## **1.13. Target Fault Restoration Time**

Target Fault Restoration Time is the expected restoration time for each component of the service.

## **1.14. Access Type**

An Access Type is the combination of Customer Premises Equipment and tail service provided by us.

## **1.15. Service Ready For Use**

A Service is deemed Ready For Use when the customer is notified by Provisioning Consultant that installation and commissioning has been successfully completed.

## **2. COMMANDER VPN DESCRIPTION**

OneStream VPN is Commander's MPLS based IP VPN product. OneStream VPN provides a wide choice of Tail Technologies, CPE, Service Levels, and Shared Services to deliver IP VPN solutions to suit customer's geographic, commercial & technical requirements. OneStream VPN supports the IP protocol only. IP Multicast is currently not supported.

### **Product Components**

The core components of OneStream VPN include:

- Shared Services
  - VPN Core
    - National MPLS Backbone
    - Provides national Points of Presence
    - MPLS based VPN Security
    - Delivers flexible QoS choices
  - Internet
  - Network Based Firewalls
- Access
  - Connects customer sites to National Backbone
  - Choice of Technologies
    - Ethernet
    - Leased Lines

- DSL
- Wireless
- Dial
- Service Levels
  - Choice of Availability Service Level
    - Standard
    - Enhanced
    - Premium
  - Choice of CPE Service Level
    - Port Only
    - Tail Only
    - Remote
    - Onsite
  - Choice of Management Service Level
    - Basic
    - Plus
  - Choice of Performance Service Levels
    - Realtime
    - Streaming
    - Interactive
    - Base
- Additional Services
  - Hosted Email
  - DNS Hosting
  - Telehousing Facilities

Each of the topics above is covered in detail in the sections below.

### 3. OneStream VPN COMPONENTS

The OneStream VPN service is made up of the following components:

<b>VPN Core</b>	The core infrastructure upon which your VPN services are deployed
<b>Access Services</b>	The customer equipment and tail service at each customer location
<b>Shared Services</b>	Refers to any Voice, Data and Internet services operating across the OneStream VPN network
<b>Additional Services</b>	Services supplied to you within the Core
<b>Service Levels</b>	The Service Levels provided with your service(s)

*Table 2 – OneStream VPN Service Components*

#### 3.1. VPN Core

The VPN Core provides the VPN functions. This core provides meshed interconnectivity between the Access connections with the appropriate QoS for each Access as specified in the Application Form. The VPN Core operates over Commander's MPLS Backbone comprised of Point of Presence (PoP) in all major capital cities and a redundant fibre infrastructure delivering network services across Australia. The VPN Core is considered to be a Shared Service

##### **3.1.1. Core Network Target Availability**

OneStream VPN provides a Core Network Target Availability of 99.95% during the Fault Coverage Hours. Core Network Faults with a severity level 1 or 2 will go toward the availability calculation for

each affected Access Service. Rebates for backbone faults are provided for under the Access Type rebate calculations.

### 3.1.2. Core Network Performance

The OneStream VPN Core supports the Service Classes and performance Guarantees as detailed in Table 3 below. The ability to send and receive information in each Service Class is controlled by the Traffic Contract you have selected for each Access.

Service Class	Latency (One Way)	Jitter	Packet Loss
Realtime	60ms	10ms	0.05%
Streaming	100ms	15ms	0.5%
Interactive	150ms	30ms	1%
Base	N/A	N/A	N/A

*Table 3 – Core Network Performance Measure*

## 3.2. Access Services

The Access Service provides the connection from the VPN Core to your premises including:

- The physical tail circuit to your premises
- Any CPE selected by you within the Service Level.
- VPN Port to provide connection to the VPN Core

### 3.2.1. Physical Tail Circuit

The physical tail circuit provides connectivity between Commander's Point of Presence and your premise. Commander supports a wide variety of Tail Circuits, including:

- Ethernet
- Leased Line
- SDSL
- ADSL
- iBurst
- Dial

The tail circuit you have selected is nominated in Schedule One of the Application Form.

### 3.2.2. CPE

Commander can optionally provide CPE to terminate the Tail Circuit and provide the interface to the network on your premises. Refer to the Service Levels section for details on CPE supply, installation & management

### 3.2.3. VPN Port

The VPN Port provides the connection from the Access to the VPN Core. The VPN Port specifies the Port Speed & Traffic Contract applicable to the Access.

### 3.2.4. VPN Port Speed

The VPN Port Speed selected by you nominates the maximum speed of traffic sent to and from your Access tail. You can select a Port speed lower than the maximum speed of the physical Tail Circuit but you cannot select a Port Speed greater than the maximum speed of Tail Circuit.

### 3.2.5. VPN Port Traffic Contract

The VPN Port Traffic Contract selected by you nominates the VPN Core Service Classes available for transmission of your traffic across the VPN Core.

Commander has five (5) Traffic Contracts, as listed in Table 4 below, to provide customers with the QoS they need for their specific application, but allow other traffic types where applicable. Each Traffic Contract provides access to the VPN Core Services Classes as described below.

Traffic Contract	Traffic Allowances	Service Class Bandwidth			
		Realtime (DSCP set to EF)	Streaming	Interactive	Base
	MPLS EXP	5	2	1	0
Dynamic 25	Maximum Bandwidth	25% Excess traffic is dropped	20% Excess traffic is carried as Base	20% Excess traffic is carried as Base	100%
	Minimum Reserved Bandwidth	25%	20%	20%	20%
	IP Precedence	7,6,5	4,3,2	1	0
Dynamic-Realtime	Maximum Bandwidth	100%			
	Minimum Reserved Bandwidth	80%	5%	5%	5%
	IP Precedence	7,6,5	4,3,2	1	0
Dynamic-Streaming	Maximum Bandwidth	0% Presented traffic is carried as Streaming	100%		
	Minimum Reserved Bandwidth	0%	80%	5%	5%
	IP Precedence		7,6,5,4,3,2	1	0
Dynamic-Interactive	Maximum Bandwidth	0% Presented traffic is carried as Interactive	0% Presented traffic is carried as Interactive	100%	
	Minimum Reserved Bandwidth	0%	0%	80%	5%
	IP Precedence			7,6,5,4,3,2,1	0
Base	Maximum Bandwidth	0% Presented traffic is carried as Base	0% Presented traffic is carried as Base	0% Presented traffic is carried as Base	100%
	Minimum Reserved Bandwidth	0%	0%	0%	100%
	IP Precedence				7,6,5,4,3,2,1,0

**Table 4 – Traffic Contract Details**

### 3.2.5.1. Service Classes

All traffic is carried across the network in one of 4 service classes. Table 5 below details the characteristics and intended purpose for each Service Class.

Service Class	Typical Purpose	Maximum Traffic Load	Recommended Tail Circuits	Recommended Minimum Port Speed
Realtime	Voice, Video, Interactive Multimedia	85% of VPN Port Speed	Ethernet, Leased Line, SDSL VBR	768kbit/s
Streaming	Streaming Voice & Video Applications	85% of VPN Port Speed	Ethernet, Leased Line, SDSL VBR	512kbit/s
Interactive	Mission Critical & Interactive Data Applications. (e.g. Telnet, Citrix, etc.)	100% of VPN Port Speed	Ethernet, Leased Line, SDSL VBR	256kbit/s
Base	Non-interactive, non-mission critical business applications (e.g. Email, HTTP, etc.)	100% of VPN Port Speed	All	All

**Table 5 – QoS Profile Provisioning**

## Realtime Service Class

The Realtime Service Class provides performance targets suitable for the carriage of interactive Voice & Video applications (e.g. Telephone Calls, Video Conferencing etc). It is recommended that Realtime traffic should not exceed 85% of the VPN Port Speed. It is recommended that the physical Tail Circuit with an Access speed greater than 768kbit/s should be chosen to provide a similar level of performance to deliver acceptable end-to-end performance. While Commander supports the use of non-Realtime tail circuits in conjunction with Realtime Service Class, Commander cannot guarantee performance levels.

## Streaming Service Class

The Streaming Service Class provides performance targets suitable for the carriage of streaming Voice & Video applications (e.g. Audio & Video broadcasts etc). It is recommended that Streaming traffic should not exceed 85% of the VPN Port Speed. It is recommended that the physical Tail Circuit with an Access speed greater than 512kbit/s should be chosen to provide a similar level of performance to deliver acceptable end-to-end performance. While Commander supports the use of non-Streaming tail circuits in conjunction with Streaming Service Class, Commander cannot guarantee performance levels.

## Interactive Service Class

The Interactive Service Class provides performance targets suitable for the carriage of mission critical & interactive business data applications (e.g. Citrix, Telnet etc). It is recommended that the physical Tail Circuit with an Access speed greater than 256kbit/s should be chosen to provide a similar level of performance to deliver acceptable end-to-end performance. While Commander supports the use of non-Interactive tail circuits in conjunction with Interactive Service Class, Commander cannot guarantee performance levels.

## Base Service Class

The Base Service Class provides a standard service for the carriage of non-time critical data applications (e.g. Email, FTP, Web Browsing etc).

### 3.2.5.2. Traffic Classification & Marking

Commander uses Differentiated Services to classify & mark IP traffic at the CPE (if the CPE is QoS capable) or the PE (if the CPE is not QoS capable). Commander has a standard template (called "Application to DSCP Mapping Table" which defines the classification of all traffic types and the DiffServ Code Points (DSCP) applied to each traffic type. IP traffic can be classified & marked at either the CPE (for QoS capable CPE) or the PE (for non-QoS Capable CPE). Customisation of QoS functions can be performed by loading customised "Application to DSCP Mapping tables in CPE where required. PE based classification & marking can only be performed in accordance with the predefined "Application to DSCP Mapping Table" template. Should the PE perform classification & marking it will overwrite the existing DSCP header and this will follow through to the customer's network.

Table 6 below details the current default traffic classification & marking configuration where traffic is classified & marked by Commander CPE or PE (for non-QoS capable CPE). Customer specific variations of the table below can be supported where customers purchase managed CPE from Commander or supply their own CPE.

Application	Protocol	DSCP	IP Precedence
VoIP bearer	RTP voice	EF	5
Voice and video signalling and control	RTCP	EF	5
	H.323	EF	5
	SIP	EF	5
Video conference	RTP video	AF21	2
Streaming video	cuseeme	AF21	2
	netshow	AF21	2
	realaudio	AF21	2
	streamwork	AF21	2
	vdolive	AF21	2
Network Management	SNMP	AF21	2
	Syslog	AF21	2

	DHCP	AF21	2
	DNS	AF21	2
	LDAP	AF21	2
	secure-LDAP	AF21	2
	socks	AF21	2
	kerberos	AF21	2
Database	SAP	AF11	1
	sqlnet	AF11	1
	sqlserver	AF11	1
	citrix	AF11	1
	notes	AF11	1
Interactive sessions	telnet	AF11	1
	secure-telnet	AF11	1
	xwindows	AF11	1
	SSH	AF11	1
	finger	AF11	1
Other enterprise applications	novadigm	AF11	1
	pcanywhere	AF11	1
File transfer	FTP	0	0
	secure-FTP	0	0
	NNTP	0	0
	secure-NTP	0	0
	printer	0	0
Email and groupware	exchange	0	0
	SMTP	0	0
	POP3	0	0
	secure-POP3	0	0
	IMAP	0	0
	secure-IMAP	0	0
Peer-to-peer file transfer	napster	0	0
	fastrack	0	0
	gnutella	0	0

**Table 6 – Current Default Traffic Classification & Marking Configurations**

Table 6 may change, and be updated, from time to time.

### 3.3. Shared Services

Services that are delivered from within the VPN Core (e.g. Network based Firewall & Network based Internet) are referred to as a Shared Service.

#### 3.3.1. Shared Service Target Availability

Target Availability for Shared Services is 99.95% during the Fault Coverage Hours each month.

### 3.4. Additional Services

#### 3.4.1. Additional Services Target Availability

Target Availability for Additional Services is 99.5% during the Fault Coverage Hours each month.

#### 3.4.2. Additional Services Features

In addition to your Commander VPN network this Service Schedule covers the Additional Services purchased in conjunction with your network. The Additional Services available under this agreement are:

- Hosted IP addresses
- Email holding queue
- Shared hosted email
- Shared hosted domain names
- Telehousing Services

Additional services are monitored as part of the Network Operation Centre on a 24x7 basis using active and passive monitoring methods.

## 4. SERVICE LEVELS

Each service in a customer network is comprised of a number of components (e.g. CPE, Tail & Network Management) so Commander has developed a simple Service Level Agreement (SLA) structure that provides the flexibility to support a wide range of technologies yet is simple to understand.

The Service Level naming structure indicates two distinct components:

### “Availability Service Level” + “CPE & Management Service Level”

These two components are combined to nominate the ‘Service Level’ for each service in the network.

Each service component is described below.

#### 4.1. Availability Service Level

The Availability Service Level indicates the coverage hours, target availability and restoration targets specific to each site. Tail Fault Coverage & Availability levels vary by technology, supplier, & geographic location so each site in a single network can have different Site Coverage & Availability levels.

Site Coverage levels include:

- Premium
- Enhanced
- Standard

The Availability Service Levels available with your service are shown below, in Table 7. The level that applies to your service is dependant on the Access Type (refer to §3.2.1) you select at each site.

	Premium	Enhanced	Standard
<b>Technical Helpdesk Hours</b>	24 x 7 x 52	24 x 7 x 52	24 x 7 x 52
<b>General Helpdesk Hours</b>	Mon-Fri, Excluding Public Holidays 8am – 8pm *		
<b>Provisioning Helpdesk Hours</b>	Mon-Fri, Excluding Public Holidays 8:30am – 5:00pm *		
<b>Telephone Response Time</b>	80% within 120 seconds	80% within 120 seconds	80% within 120 seconds
<b>Fault Response Time</b>	30 Minutes	30 Minutes	30 Minutes
<b>Fault Coverage Hours</b>	24 x 7 x 52	8am-8pm, Mon-Sat, Excluding Public Holidays †	8:30am-5:00pm, Mon-Fri, Excluding Public Holidays †
<b>Target Availability</b>	99.90%	99.70%	99.50%
<b>Target Fault Restoration Time (Metro/CBD)</b>	4 Hrs	10 Hrs	18 Hrs
<b>Target Fault Restoration Time (Regional)</b>	6 Hrs	20 Hrs	24 Hrs
<b>Rebates For Metro/CBD Services</b>	>4Hrs<6Hrs = 15%	>10Hrs<20Hrs = 15%	>18Hrs<24Hrs = 15% (OnsitePlus only) *
	>6 Hrs = 30%	>20 Hrs = 30%	>24 Hrs = 30% (OnsitePlus only) *
<b>Rebates For Regional Services</b>	>6Hrs<8Hrs = 15%	>20Hrs<24Hrs = 15%	>24Hrs<36Hrs= 15% (OnsitePlus only) *
	>8Hrs = 30%	>24Hrs = 30%	>36Hrs = 30% (OnsitePlus only) *

\* Refers to Australian Eastern Standard Time (AEST)

† Public Holidays are as defined in the location where the fault occurs.

‡ If SLA denotes "Excludes Line" then the SLA does not include faults on any underlying telephone line

\* SLA Rebates do not apply for Standard Onsite, Standard Tail Only or Standard Port Only services

*Table 7 – Availability Service Level Details*

## 4.2. CPE & Management Service Level

This indicates who provides, installs, maintains and manages the CPE at that site. Each site in a single network can have different CPE & Management levels. CPE Service level varies by Access technology and supplier so not all CPE levels are available for each Access type. CPE Service Levels include:

- Port Only - Commander does not supply the Tail or any CPE. Access to the Commander Backbone is via an IPSec session over customer supplied Tail Service.
- Tail Only - Commander does not supply the CPE. The customer is responsible for supplying the CPE and interfacing it with the Tail circuit.
- Remote - Commander supplies preconfigured CPE for the customer to install. In the event of CPE failure, Commander will ship a replacement unit to the customer. The customer can also request onsite attendance by a Commander technician but this will be chargeable at the applicable Fee For Service rates.
- Onsite - Commander supplies the CPE, including installation and onsite maintenance.
- OnsitePlus – Commander supplies, installs & maintains the CPE plus provides proactive management & online reporting where available

Table 8 illustrates the options included for each CPE & Management Service Level.

	Port Only	Tail Only	Remote	Onsite	OnsitePlus
CPE Supply	No	No	Yes	Yes	Yes
Configuration	No	No	Yes	Yes	Yes
Installation	No	No	No	Onsite	Onsite
Hardware Replacement	No	No	Yes	Onsite	Onsite
CPE Config Maintenance	No	No	Yes	Yes	Yes
Project Management	No	No	No	No	Yes
Fault Detection & Notification	Reactive	Reactive	Reactive	Reactive	Proactive
Included Moves & Change	No	No	No	No	Yes
Monitoring (IP Polling)	No	No	No	No	Yes
Performance Reporting	No	No	No	No	Yes
Detailed Network Diagrams	No	No	No	No	Yes
SLA Calculation & Reporting	No	No	No	No	Yes

*Table 8 – Management Service Level Details*

### 4.2.1. CPE & Management Service Components

**CPE Supplied by Commander** – Commander provides and installs the Access Service CPE.

**Configuration** – Commander technical staff will configure your CPE to provide the specific required service characteristics.

**Installation** – Commander will provide Onsite personnel to ensure the CPE is correctly installed and provisioned.

**Hardware Replacement** – Commander will provide a replacement piece of CPE; for *Remote* Service Level the replacement unit will be shipped to the customer site. For *Onsite* Service Level a Commander technician will deliver and install the replacement CPE at the customer's site.

**CPE Config Maintenance** – Commander maintains a current copy of the customer's CPE configuration.

**Fault Detection** – Proactive monitoring of a customer network is available as a Plus level Service. Reactive monitoring is provided for all other Service Levels.

**Monitoring (IP Polling)** – As part of the Proactive monitoring service all customer CPE elements are routinely polled (at approx. 10 minute intervals) using the Ping protocol.

**Performance Reporting** is provided through Commander's Web Portal.

**Detailed Network Diagrams** are included as part of your *OnsitePlus* Service Level Project Management service.

**SLA Calculation & Reporting** are also part of the Project Management service.

#### **4.2.2. Project Management**

**Project Management** - Any Access Service ordered with a *Plus* Service Level will be assigned a Project Manager. The Project Manager will carry out the tasks outlined below as agreed:

- Installation co-ordination and migration planning
- Project milestone & progress reporting
- Escalation and problem management
- Service design and consulting
- Configuration enhancements
- Add/Moves/Changes

#### **4.2.3. Minor Add or Change**

All Plus Service Level agreements include up to One Business Man-hour of Provisioning resource for any minor Add or Change requirements. These requests must be made during the Provisioning Helpdesk Hours and use Commander personnel. Up to one hour of work (per month) is included in a minor move or change. Commander retains the absolute right to determine what is classified as a minor change.

##### **4.2.3.1. Excluded Adds and Changes**

The following work is excluded from a minor add or change:-

- Any alteration that is estimated to take longer than one hour to complete;
- Work outside the Provisioning Helpdesk Hours;
- Any alteration that incurs direct external cost to Commander;
- Any change that is part of an Additional Service.

#### **4.2.4. Reporting**

##### **4.2.4.1. Reporting Features**

The OneStream VPN service provides the following reporting as part of the service.

- Internet Usage – Available Online through Commander Web Portal
- Access Performance Reporting – Available Online to *Plus* Service customers through Commander Web Portal

##### **4.2.4.2. Reporting Target Availability**

The Target Availability of management reports is excluded from the Target Availability of the service. Management reporting information is a guide to the performance of your service and we do not warrant the reports to be accurate or available at all times.

The username and password to access the website reporting functions will be included in your service Welcome Pack information. If you need to obtain a new password please contact the General Help Desk to arrange a new one.

## 5. ADDS, MOVES & CHANGES

Commander understands that adds, moves & changes (AMCs) are necessary throughout the life of the contract and has developed a flexible structure to support the changing needs of any network. These changes supported are detailed in Table 9 below:

AMC Type	Contract Impact	Pricing Impact
Addition of New Site	Each Site is individually contracted. New sites can be added to existing network but contract minimum term applies to each site	Each Access is priced individually. Addition of one access simply increases network price by that amount but contract amount is sum of contracted services.
Access Speed Change	Some tail types can support a speed change. Where supported, the speed change has no impact on service contract.	Upfront charge to implement speed change plus change to monthly recurring charge
Access Relocation	Some tail types can be relocated but some can't due to technical reasons (e.g. no service coverage at the new location). If the service can be relocated, then a new contract term applies to the relocated access. If the existing tail can't be relocated (e.g. no coverage) then the existing access can be cancelled as an Early Termination and a new service can be installed at the new site	Upfront Relocation Charge (where supported)
Access Change (Technology Change)	Some tail types can be converted to other technology but some can't due to technical reasons. If the service can be converted, then a new contract term applies to the converted access. If the existing tail can't be converted, then the existing access can be cancelled as an Early Termination and a new service can be installed.	Upfront Service Change Charge (where supported)
Cancellation of Existing Site	Each Site is individually contracted. Sites can be removed from the network without impacting other sites.	Early Termination Payment applies. <ul style="list-style-type: none"> <li>• 100% of the remaining Minimum Monthly Spend (contracted value for the service being terminated) if termination is within 12 months of commencement of the Minimum Term</li> <li>• 50% of the remaining Minimum Monthly Spend (contracted value for the service being terminated) if termination is after 12 months of commencement of the Minimum</li> </ul>
Change of Configuration	Nil	Once-Off Charge
Chargeable Site Visit	Nil	Once-Off Charge
Chargeable Fault Call	Nil	Once-Off Charge
Failed Site Visit	Nil	Once-Off Charge
Non-Return of Hardware	Nil	Once-Off Charge
Service Reconnection	Nil	Once-Off Charge

*Table 9 – Supported Adds, Moves and Changes*

## 6. PROVISIONING

The length of time taken to provision or make changes to an Access Service is related to the Access technology used.

### 6.1. Access Service Provisioning & Relocation Lead Times

Provisioning & Relocation Lead Times begins when we accept your order, except where your Access Service is scheduled to begin at a later date as agreed.

#### 6.1.1. Provisioning Outside Of Provisioning Helpdesk Hours

We are able to arrange for the installation of Access services outside of the standard Provisioning Helpdesk Hours on a time and materials basis.

### 6.2. Access Service Adds and Changes Lead Time

The Adds & Changes Lead Time begins when we accept your order except where scheduled to begin at a later date as agreed.

### 6.3. Target Lead Times

Provisioning and Relocation lead time shown in Table 10 are assuming physical network infrastructure is already present in customer premise.

Access Type	Technology Type	Provisioning / Relocation (Metro/CBD)	Provisioning / Relocation (Regional)	Adds & Changes
Ethernet	Fibre	25 days	Upon Application	5 days
Leased Line	DAR, E1, X.163	20 days	40 days	10 days
DSL	ADSL, SHDSL, HDSL	20 days	30 days	5 days
Dial	ISDN	10 days	20 days	5 days
Dial	PSTN	5 days	5 days	3 days

*Table 10 – Target Provisioning, Relocation, Adds and Changes Lead Times*

## 7. FAULT REPORTING

To log a fault with the Technical Helpdesk please call the General Helpdesk number on your bill and choose “Technical Helpdesk” from the options available. To avoid any delay in resolving a fault you must log faults with the Technical Helpdesk. If you do not log a fault with the Technical Helpdesk the fault will be excluded from any availability and rebate calculations.

To ensure we are able to log your fault please quote the following information when contacting the Technical Helpdesk:

1. The affected Service (including Service Number or Service ID - which can be found in your Welcome Pack)
2. A description of the fault
3. The name and phone number of the person in your organisation who will accept the response call

### 7.1. Fault Classification

Faults are classified for the purposes of calculating rebates as shown in Table 11 below:

Severity	Example fault
1	Customer network, tail or CPE unavailable affecting individual or multiple sites/locations.
2	CPE or network performance impaired whilst most business operations remain functional.
3	Intermittent loss or degradation of service (resolved as no fault found by us).
4	Configuration change or feature enhancement required.

*Table 11 – Fault Classifications*

## 7.2. Fault Response Time

Once you have logged a fault with the Technical Helpdesk the person nominated will receive a response call within 30 minutes with an update of the progress of the fault. Further updates on the fault progress will be given to the nominated contact every 2 hours after the initial response.

Where a fault of severity level 1 has been detected automatically we will call your nominated contact to confirm the validity of the fault. All automatically detected severity level 1 faults will be logged on our fault ticketing system when we begin work on resolving the fault.

For all other automatically detected faults we will respond within 30 minutes to the nominated contact recorded in our systems to advise of the status of the fault. Further updates on fault progress will be given to the nominated contact every 2 hours after the initial response.

## 7.3. Outage Notification

We aim to provide at least 5 working days notification of any scheduled outage where the outage may affect your service. Where practical a scheduled outage will occur between 1am and 5am. Commander has a regular maintenance window on Sunday between the hours of 1am and 5am and will schedule maintenance during this period whenever reasonable to do so.

In circumstances where an emergency service interruption is required, we reserve the right to undertake the service interruption at shorter notice. In such cases we will use best efforts to notify you prior to the service interruption.

## 8. REBATES

NOTE: In order for an SLA rebate to be processed a *Rebate Request Form* must to lodged.

Rebates are calculated based on the Unavailable Hours. OneStream VPN provides rebates on Access, Shared Services and Additional Service components of your service.

Rebates	Premium	Enhanced	Standard
Services Rebates (Metro/CBD)	>4Hrs <6Hrs= <b>15%</b> >6Hrs= <b>30%</b>	>10Hrs <20Hrs= <b>15%</b> >20Hrs= <b>30%</b>	>18Hrs <24Hrs= <b>15%</b> >24Hrs= <b>30%</b> (OnsitePlus only)
Services Rebates (Regional)	>6Hrs <8Hrs= <b>15%</b> >8Hrs= <b>30%</b>	>20Hrs <24Hrs= <b>15%</b> >24Hrs= <b>30%</b>	>24Hrs <36Hrs= <b>15%</b> >36Hrs= <b>30%</b> (OnsitePlus only)

*Table 12 – Access Type Rebates*

### 8.1. Access Type Rebates

The rebate is calculated on the monthly fee for the Access Type affected in accordance with the rebates as shown in Table 12.

### 8.2. Shared Services Rebates

The rebate for Shared Services is calculated on the monthly fee for the Shared Service affected in accordance with the rebates as shown in Table 12.

### 8.3. Additional Services Rebates

The rebate, where appropriate, is calculated on the monthly fee for the Additional Service affected in accordance with the rebates as shown in Table 12.

### 8.4. Rebate Claims

Applications for rebates must be made on the 'Rebate Request Form' supplied to you by the Commander Support Representative at the time of the rebate claim.

## 9. FAULT DETECTION & MANAGEMENT PROCESS

### 9.1. Reactive Fault Detection

Services with a Fault Detection Level of 'Reactive' require the customer to report any faults to Commander's Support Helpdesk. Commander will not proactively detect faults on these services but will provide fault diagnosis and repair after the customer has reported the fault to the Support Helpdesk.

### 9.2. Proactive Fault Detection

Proactive fault detection includes active monitoring of the customer's network using a number of methods to allow detection of a service failure and begin working on it before the customer may even be aware of the fault. Where proactive fault detection is provided we use Active Network Monitoring via:

- Online SNMP or ICMP polling of network devices at 10 minute intervals.
- The collection and analysis of SNMP traps from all managed devices is performed by our HP Openview management system.

Once a fault has been detected a Service Order is logged into our Trouble Ticketing database and we will notify the customer according to the schedule below:

#### 9.2.1. Notification for Proactively Detected Faults

The following Notification Schedule table defines how customers will be contacted for faults proactively detected on 'Plus' level services.

Table 13 below is an excerpt from your Welcome Pack, your preferred out-of-hours notification contact details shall be provided to Commander at the time of contract signing.

Notification Schedule	
<b>Within SLA Fault Coverage Hours</b>	
1st Attempt	> Ring primary contact via business landline and/or ring primary contact via mobile.
2nd Attempt	> Ring site/secondary contact via business landline and/or ring site/secondary contact via mobile.
3rd Attempt	> Email and SMS primary contact and secondary contact, if attempts 1 and 2 are unsuccessful
<b>Outside of SLA Fault Coverage Hours (see NOTES:)</b>	
<input type="checkbox"/>	Contact using schedule above
<input type="checkbox"/>	Don't contact outside of Fault Coverage Hours. Send email to primary contact only.
<b>For Premium Plus Sites</b>	
<input type="checkbox"/>	Don't contact between 9pm to 6am

**NOTES:** Where a fault is identified outside of fault coverage hours, a fault will be logged into our Fault Management system. Please note that we may choose to work on the fault outside of the fault coverage hours; however this will be done at our discretion.

Where a landline or mobile diverts to a message-bank system, a message will be left and we will continue with all 3 contact attempts.

*Table 13 – Notification Schedule*

#### 9.2.2. Action

Faults that are detected by the DSC network management systems will be actioned by the DSC engineer immediately upon detection. The DSC engineer will remotely analyse these alarms by the use of dedicated management software for the device affected. This software provides the ability to diagnose the location and cause of the fault.

Resolution of the problem would normally be performed remotely via use of the remote management software. However, where a problem cannot be resolved by the DSC, the service

order is passed to the Commander Customer Support Level 2 team. If the problem is not resolved within the pre-defined escalation parameters, a Customer Support Engineer will be dispatched to site. The DSC staff will continue to monitor the trouble ticket and update the customer on the progress of the fault.

### **9.2.3. Regular Updates**

The Availability Service Level details the frequency of updates provided when a fault has been logged on a service. Updates will be made via phone to the contact recorded on the Service Order, or can be made via email if requested at the time of reporting.

## **10. CONTACT DETAILS**

Refer to your OneStream VPN Welcome Pack for all your Account Management contacts and Support numbers.