ans

Service Definition

Cloud Gateway | Managed

1. Operational Services

1.1 Service Description

Normal Business Hours = 9:00 -17:30, Monday to Friday
(excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

1.1.1 ANS Service

Service	Service Description	Service Hours
Incident Management		
Service Desk - Non Business Critical Faults	The Supplier provides access with relevant phone and email contact details to the Supplier Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4).	Normal Business Hours
Service Desk - Business Critical faults	The Supplier provides 24/7 access with relevant phone contact details to the Supplier Service Desk for critical system down scenarios (P1) only.	24 x 7
Priority Escalation to Carrier or Vendor for faults	Priority escalation to Carrier (P2/P3/P4).	Normal Business Hours
High Priority Escalation to Carrier or Vendor for Faults	High Priority escalation to Carrier or Fortinet Support for Priority 1 (P1) business critical faults.	24 x 7
Change Management & Advisory		
Access Control List Configuration & Management	The supplier will configure and manage Access Control Lists to suit your requirements via change management	Normal Business Hours
NAT Configuration & Management	The supplier will configure and manage inbound and outbound Network Address Translation (NAT) rules to suit your requirements via change management	Normal Business Hours
VPN Configuration & Management	The supplier will create, configure and manage VPN configurations.	Normal Business Hours
Routing Changes	The supplier will provide Change Management for Static and Dynamic routing changes	Normal Business Hours
Security Profile		
Intrusion Prevention System	Where the Intrusion Prevention System (IPS) is licensed the Supplier will deploy and manage required policies	Normal Business Hours
Application Control	Where Application Control is licensed the Supplier will deploy and manage required policies	Normal Business Hours
Antivirus	Where Antivirus is licensed the Supplier will deploy and manage required policies	Normal Business Hours

Web Filtering	Where Web Filtering is licensed the Supplier will deploy and manage required policies	Normal Business Hours
Malware	Where Malware is licensed the Supplier will deploy and manage required policies	Normal Business Hours
High Availability & Recovery		
HA Configuration	Where a high-availability solution has been deployed the Supplier will configure and manage the failover to standard specifications	24 x 7
Failover Management & Recovery	Where a high-availability solution has been deployed, the Supplier will help manage switchover during failure.	24 x 7
Monitoring & Event Management		
Platform Monitoring	• Availability Monitoring • Intrusions Blocked and Detected where licenced • Viruses Blocked and Detected where licenced • HTTP Requests / Sessions /URLs Blocked where licenced • Traffic monitoring and Statistics	24 x 7
Alert Configuration and Response	The Supplier will configure Alerts for the environment and respond to Alerts. Alerts will be handled as Incidents within the Incident Management process	Normal Business Hours
Service Operations		
GLASS Portal Access	Customer access to ANS GLASS portal providing visibility of all Service related tickets, alerts and performance dashboards.	24 x 7
Problem Management	ANS Problem Management processes are adhered to for incident, change and event reduction. Problems are reviewed during the Service Management Review.	Normal Business Hours
Service Reviews	Service Management Review (SMR) Reports will be distributed at regular intervals and discussed via a meeting between the Supplier and the Customer. The SMR Report will cover the previous period. Please refer to your Service Statement for SMR frequency and meeting type.	Normal Business Hours
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. Where applicable a Service Disruption Report will be created.	Normal Business Hours
Change Management Process	The Supplier will take full ownership of the Change Management Process for the Customer Supported Assets.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes.	24 7

1.2 Incident Management

1.2.1 Incident Priority Table:

Affect	Business Impact		
	Minor	Moderate	Major
System/Service Down	P3	P2	P1
System/Service Affected	P4	P3	P2
User Down/Affected	P5	P4	P3

1.2.2 Incident Response and Escalation Table:

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	30 Minutes	2 Hours	Immediate	Immediate	Hourly Email	6* hours
P2	1 Hour	4 Hours	1 Day	None	GLASS Portal	2 Days
P3	4 Hours	2 Days	4 Days	None	GLASS Portal	10 Days
P4	1 Day	Never	Never	None	GLASS Portal	30 Days
P5	2 Days	Never	Never	None	GLASS Portal	None

For an Incident, “Response” is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call or in person. For detailed process flow see the current Managed Services Handbook. Support to provide a resolution shall be provided within Service Hours from the time of Response until the Incident has been resolved.

From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in the table above.

*Resolution KPI is subject to change dependant on Partner availability.

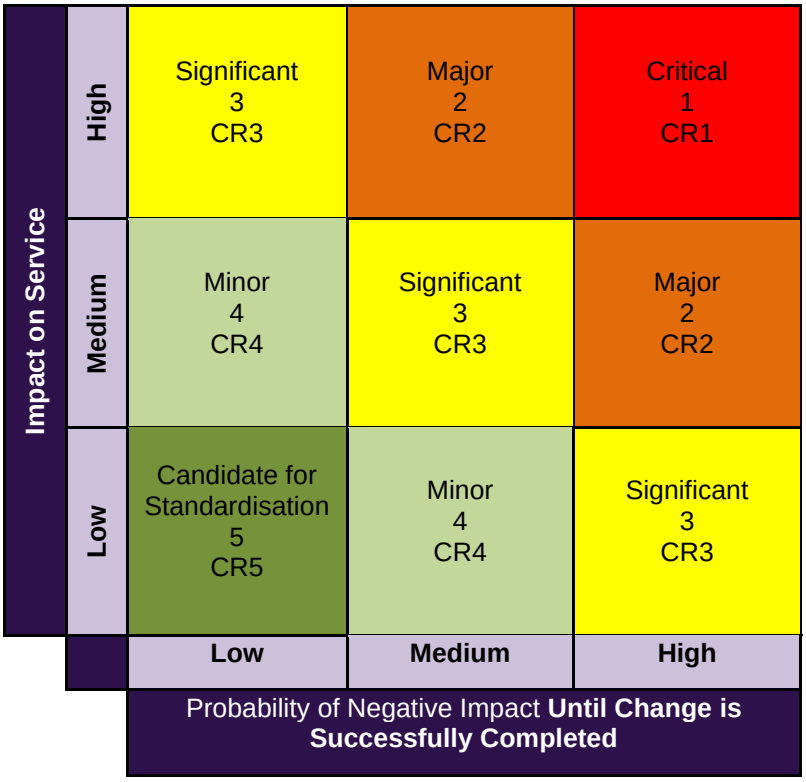
1.3 Change Management

All Changes require a Request for Change (RFC) form to be completed on the Suppliers GLASS Portal and submitted detailing the required Change. The Supplier will reject unapproved or incomplete RFC forms.

Changes will follow the Change Management Process as defined in the ANS Managed Services Handbook. It should be noted that Emergency Changes will only be carried out in the event of a P1 scenario (either pro-active or reactive) and/or a major Security Incident where the Supplier deems appropriate.

.

1.3.1 Change Risk Assessment Matrix



1.3.2 Change implementation targets Table:

Change Type	Implementation Start Date
Normal CR1	1 Working Day from CAB Approval
Normal CR2	2 Working Days from CAB Approval
Normal CR3	3 Working Days from CAB Approval
Normal CR4	4 Working Days from CAB Approval
Normal CR5	5 Working Days from CAB Approval
Normal CR6	Project Changes (Informational and Approval only)
Standard	Change to be completed within 4 Working days from logging on ANS ITSM Tool
Emergency	Change to completed in conjunction with Incident Management Process (P1)

Emergency Changes are dealt with in conjunction with the Incident Management Process; further details of this and all other change types are detailed within the Managed Services Handbook.

Standard and Emergency Changes to the Service within the scope of this Contract will be completed by the Supplier at no additional cost.

2 Service Levels, Key Performance Indicators and Service Credits

Category	Service Level Target	Minimum Service Level	Service Credits
P1 Incidents	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.	100%	1st incident missed response time – 5% Service Credit 2nd incident missed response time – 10% Service Credit
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.	Service credits apply from 2nd failure within a calendar Month	1st incident missed response time – 0% Service Credit 2nd incident missed response time – 5% Service Credit 3rd incident missed response time – 10% Service Credit
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.	80%	<80% - 5% Service Credit
P4 Incidents	100% of Incidents responded to within 1 Working Day.	None	No Service Credit
P5 Incidents	100% of Incidents responded to within 2 Working Days.	None	No Service Credit
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution	None	No Service Credit

CR1 Change	100% of Changes start implementation within 1 Working Day from CAB Approval	100%	1 Change Missed Implementation time - 5% Service Credit 2 Changes missed Implementation times - 10% Service Credit
CR2 Change	90% of Changes start implementation within 2 Working Days from CAB Approval	85%	5% Service Credit
CR3 Change	90% of Changes start implementation within 3 Working Days from CAB Approval	None	No Service Credit
CR4 Change	90% of Changes start implementation within 4 Working Days from CAB Approval	None	No Service Credit
CR5 Change	90% of Changes start implementation within 5 Working Days from CAB Approval	None	No Service Credit
Standard Change	100% of changes implemented within 4 Working Days	90%	5% Service Credit
Site Availability	100%*	99.0%*	Pass through Carrier Service Credit where applicable

Service Credits are calculated as a percentage of the monthly Base Charge and in any event, shall not exceed 10% of the monthly Base Charge in the month that the Service Credit arose. Where a Service Credit is due it shall not accumulate with any other Service Credit and only one Service Credit can be offered within the monthly period.

Service Credits may be applicable for sub-elements of the network service only where the Supplier has been provided with a Service Credit by the third party communication's supplier (carrier).

*Service Availability - A site is classed available if a ping is successfully transmitted and received between the site managed CPE(s) and the ANS EMS. Availability is calculated utilising the following formulas:

Agreed Service Time: AST = 24*7-(SW+M)

Availability:

$$A = \frac{AST - Downtime}{AST} * 100$$

Key:
Agreed Service Time (AST)
Scheduled Work (SW)
Planned Maintenance (M)

3 Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the Terms and Conditions should be consulted.

a. Issues resulting from misconfiguration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets
c. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets
d. End User or 1st Line support
e. Technical Advice to any persons not listed as a Named Contact
f. Failure to meet Availability SLA due to local environmental factors such as power and cooling
g. Failure to meet Availability SLA where site in question has no resiliency (single circuit site)
h. Normal Changes requiring more than 2 hours of implementation time are excluded from the service and will be subject to Additional Service Charges
i. Project Changes (Normal CR6) are excluded from the service and will be subject to Additional Service Charges. Project Changes are recorded within the Supplier ITSM Tool for Informational and approval purposes only.
j. Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges
k. Changes outside of Normal Business Hours will be subject to Additional Service Charges

4 Customer Responsibilities

Including but not limited to:

a. The Customer shall have an established end user support function that may be validated by the Supplier
b. Where required, the Customer shall make available appropriately skilled Employed persons while an Incident is being managed
c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
    a. Affected Services
    b. Business Impact
    c. Number & Type of users affected
    d. Recent changes on Supported Assets (regardless of perceived impact)
    e. Environmental checks including knowledge of Building or Road works
    f. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected (where required).
    g. The Customer shall check the LED status of equipment onsite (where required)
d. The Customer shall provide full Cloud access to all Customer Supported Assets if/when required
e. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed
f. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have (where required) Supplier recommended hardware and vendor support in place.
g. The Customer is responsible for all configuration backups outside of the Supported Assets without exception.
h. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process
i. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook
j. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier)
k. The Customer shall ensure 24x7x365 availability of a suitable Escalation Contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions
l. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
m. The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Assets and/or Supplier Assets from the address specified in the Contract. Any asset that has been moved without notification to ANS may be subject to Additional Service Charges.
n. During investigations into a potential a hardware or software fault it may be required to reseat certain elements of the device/infrastructure onsite or require a device inspection for LED status. This task sits with the Customer (unless the Supported Asset is located within the Suppliers Data Centres).
o. If the Customer requires the Supplier to provide onsite hands and eyes support then this will be subject to Additional Service Charges.

It should be noted that the Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels or Service Credits for Business-Critical Incidents (P1) raised via email or GLASS Portal.

5 Assumptions

a. All Customer Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date
c. All Customer specific pre-requisites have been completed before contract commencement
d. The Customer will provide a suitable specification platform, operating system and connectivity for the Enterprise Monitoring collector server

6 Pre Requisites

a. On-Boarding Health Check and Documentation
b. Deployment of ANS Monitoring and Tooling
c. Platform and where applicable SSH, SNMP & WMI access for all monitored devices
d. Administrative Access Permissions for ANS Engineers on supported Accounts and Customer Supported Assets