Service Definition

Co-Managed Cloudflare

1. Operational Services

1.1. Service Description

The ANS Co-Managed Cloudflare offering is designed to provide customers with an easy-to-use and robust set of tools to improve website performance and protection, without compromising speed or user experience. The service makes use of a global network performance and security platform to provide protection against cyber threats such as DDoS attacks and bot attacks, while also providing performance enhancements such as a content delivery network, load balancing and enhanced DNS services.

1.2. SLA's

The ANS Co-Managed Cloudflare service is typically sold as a bolt-on alongside other managed services. Where there is an existing managed service in place, the existing SLA's will apply to the Co-Managed Cloudflare service. Where there is not an existing ANS managed service, the default SLA's will apply.

1.2.1. ANS Service

Service	Service Description	Service Hours
Incident Management	The Supplier is responsible for conducting incident management via; ANS Glass, Telephone, Teams, Email, and Remote Connection. This includes Priority 1 scenario support 24x7x365 and Priority 2-5 support in normal business hours.	P1: 24 x 7 P2-5: Normal Business Hours
Problem Management	The Supplier's Problem Management processes are adhered to for Enhancement Requests, Bug Remediation and Root Cause Analysis, post major incident. The Supplier conducts proactive problem management to identify and rectify recurring incident triggering and trend analysis. Problems are reviewed during the Service Management Review.	Normal Business Hours
Change Management	The Supplier will take full ownership of the Change Management Process for the Customer Supported Assets. Following a Security Incident or Business Critical Incident ANS will implement Emergency Changes, including expedited Cloudflare setup.	Normal Business Hours Emergency: 24 x 7
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken to identify the underlying cause. Where applicable a Service Disruption Report will be created.	Normal Business Hours

Implementation		
Initial Setup	The supplier will conduct the initial deployment of the Cloudflare Account. Additional support can be provided for the creation of domain name and addition of DNS records, upon request. Support can be provided for the initial required configuration will be applied for the suite of Cloudflare services.	Normal Business Hours
Change Management & Advisory		
Core DNS	Upon request, the supplier will implement configuration changes to CNAME zones and add/remove/update DNS records.	Normal Business Hours
Web Application Firewall	Upon request, the supplier will implement configuration changes to Web Application Firewall rules (max 100), user agent rules and add/remove/update IP access rules. In the event of false positive blocks, an engineer will review and update the configuration as necessary.	Normal Business Hours
Certificates	Upon request, if the customer is utilising their own certificates, the supplier will apply renewed certificates.	Normal Business Hours
Monitoring & Event Management		
Real time alerting	The supplier will proactively monitor Cloudflare deployments and provide alerts regarding detected and mitigated DDoS attacks.	24 x 7
In Progress DDoS Attack	During a live DDoS incident, the suppliers specialist engineers will assist in mitigating and reducing the effects of the live attack. The engineer will enable "Under attack mode" and implement any other mitigating configuration such as additional Web Application Firewall rules.	24 x 7
Customer Success		
Service Management Reporting	Service Management Reporting will be distributed at regular intervals upon request by the customer. The Report will cover the previous period.	Ad hoc
Glass Portal Access	The Customer will be given access to ANS Glass portal providing visibility of all Service-related tickets, alerts and performance dashboards.	24 x 7

1.3. Incident Management

1.3.1. 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

1.3.2. Incident Response and Escalation Table:

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	1 Hour	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	2 Hours	2 Hours	4 Hours	None	GLASS Portal	1 Day
P3	24 Hours	1 Day	2 Days	None	GLASS Portal	10 Days
P4	24 Hours	Never	Never	None	GLASS Portal	30 Days
P5	24 Hours	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.

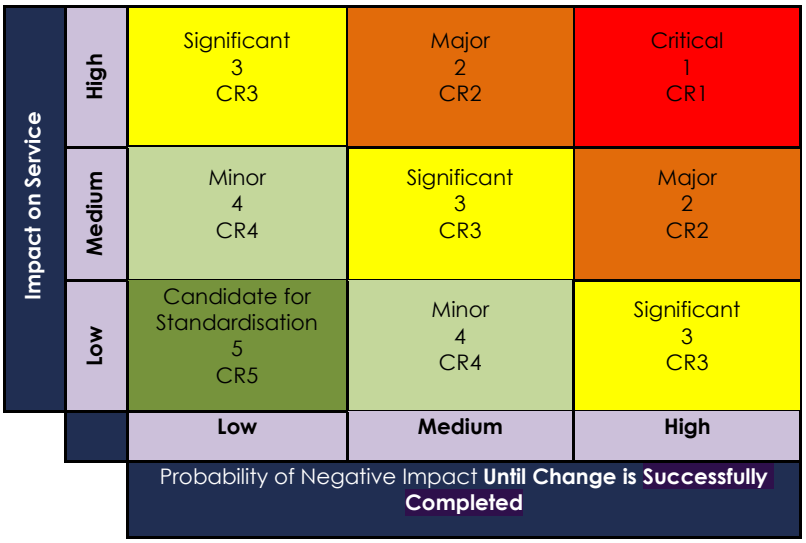
From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or Glass Portal updates at such frequencies as set out in the table above.

1.4. 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.

1.4.1. Change Risk Assessment Matrix



1.4.2. Change implementation targets Table:

Change implementation targets are based on the above priority matrix, the specific response times for each priority are defined in the exiting ANS managed service contracts and service definitions.

2. Usage/tiering

The cost of the Co-Managed Cloudflare service is based on consumption and usage of the associated services. The service cost is therefore governed by a tiering structure. Usage beyond a tier will require a move to a higher tier and, subsequently, a cost increase.

Tier 1 is defined as:

- 1 Enterprise Primary Domain
- 0.5 TB of CDN/DDoS/WAF Data Transfer
- 25 MM Requests of CDN/WAF Requests
- 25 MM DNS Queries of Foundation DNS per domain

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 Demarcation Zone resulting in impact to the Customer Supported Assets.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Demarcation Zone 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 SLA due to provider outages.

g. Normal Changes requiring more than 2 hours of implementation time are excluded from the service and will be subject to Additional Service Charges,
h. Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges E.g. Poor planning from a Customer Managed Project.
i. Performance issues outside of business hours.
j. The Fair Usage Policy applies to this service.
    a. Daily requests for a period of greater than 5 days
    b. Support requests taking in excess of 30 minutes to complete will be chargeable.
    c. Charges for excessive usage will be calculated at our standard hourly rate which can be found within the Managed Services Handbook.
k. Expedited setup of Cloudflare, outside of business hours, requires an active major incident and subsequent approval from the Major Incident Manager.

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)
d. 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.
e. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced.
f. The Customer is responsible for all data and configuration backups without exception. The Supplier does not backup any Customer data.
g. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process.
h. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook.
i. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier).
j. 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.
k. 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.
l. 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 raised via email.
m. The Customer must be able to provide the Supplier with accurate application and services information in order for the Supplier to successfully on-board the service.
n. The Customer must provide written confirmation that they accept the charges related to the Cloudflare setup and subsequent Managed Service, prior to the setup, for an expedited setup during a major incident.

5. Assumptions

a. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.
b. All Customer specific pre-requisites have been completed before contract commencement.
c. The Customer will provide resource to work with the Supplier to on-board the service.

6. Pre-Requisites

a. Customers must have a registered domain name. Cloudflare acts as a proxy.
b. Customers websites must be hosted, Cloudflare does not host content itself.
c. Customers must have administrative access to their domains DNS settings so that nameservers can be updated to point to Cloudflare's nameservers.
d. Customers must be able to use Cloudflare's SSL certificates or alternatively provide their own.