Service Definition

Managed Patching

1. Operation Services

1.1. Service Description

ANS' Managed Patching Service will ensure you have a consistently configured environment that is secure against known vulnerabilities in your operating system.

Operating system patching requires a high standard of maintenance and administration to ensure patch compliance across your operating system estate, as well as flexibility during periods of growth and change.

Managed Patching will provide you with a service which utilises a number of toolsets to ensure patch compliance of server endpoints across Azure, AWS and on-Premises infrastructure, as well giving you access to our experienced engineers to tailor-make workflows for scheduling and handling automated patch distribution to servers.

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	The Supplier is responsible for conducting incident management via, 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 and Bug Remediation and Root Cause Analysis. The Supplier conducts proactive problem management to identify and rectify recurring incidents 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.	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. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken	Normal Business Hours

	to identify the underlying cause. Where applicable a Service Disruption Report will be created.	
Patch Management	The Supplier shall patch Supported Assets in line with the agreed schedule. Assets are grouped in weekly cycles and the process is repeated monthly. Monthly Patch Status Report of all assets within the patching cycle under the ANS service. Zero Day Patch release service in the event of an urgent zero-day patch being released, the Supplier will push out the patch via an Emergency Change process upon agreement by the Customer.	24 x 7
Platform Monitoring	The Supplier will monitor the platform providing bespoke workflows, thresholds, availability and performance. Access to the Enterprise Monitoring solution will be provided to the Customer via ANS Glass and direct monitoring portal access.	24 x 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	1 Hour	Immediate	Immediate	Hourly Email	4 hours
P2	1 Hour	2 Hours	4 Hours	None	GLASS Portal	1 Day
P3	4 Hours	1 Day	2 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

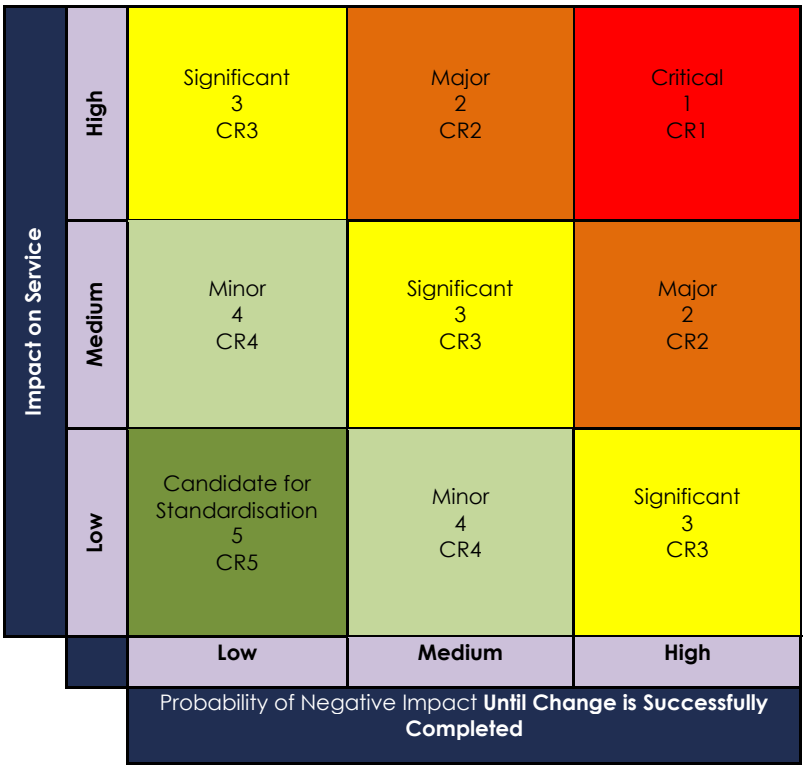
For an Incident, "Response" is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, Glass Portal update, telephone call or in person. For detailed process flow see the current Managed 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.

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
Patch Compliance	90% of critical patches implemented within 1 month of patch release	90%	5% Service Credit

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.

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 local environmental factors such as power and cooling.
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. 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.
i. 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.

j. Patching of Customer Supported Assets that do not comply with vendor best practices and configurations.
k. Desktop Operating Systems.
l. Server Operating System upgrades.
m. Escalation to Microsoft Premier Support is limited to Major incidents, subject to Major Incident Manager approval. Escalation of Sev B or lower cases is subject to additional 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. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected
    f. The Customer shall check LED status of equipment where required onsite
d. The Customer shall provide full physical access to all Customer Supported Assets at Customer Premises 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 Supplier recommended hardware and vendor support in place.
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. 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 will be subject to Additional Service Charges.
m. During investigations into a potential 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).
n. If the Customer requires the Supplier to provide onsite hands and eyes support, then this will be subject to Additional Service Charges.
n. 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.
o. The Customer is responsible for the sign-off of each patch cycle ensuring User Acceptance Testing (UAT) has been completed. Without feedback the UAT process is assumed accepted by the Customer and patching will progress by the Supplier.

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. Customer Network connectivity will be maintained to enable the Supplier access to Supported Assets for the delivery of the Service including remote diagnostics for faults.
e. The Customer will provide a suitable specification platform, operating system for the Enterprise Monitoring collector server.
f. The Customer will provide resource to work with the Supplier to on-board the service.

6. Pre-Requisites

a. On-Boarding Health Check and Documentation.
b. Platform and where applicable WMI access for all patching services.
c. A centralised authentication solution such as Active Directory or other directory-based identity related service is available to manage Windows based operating systems.