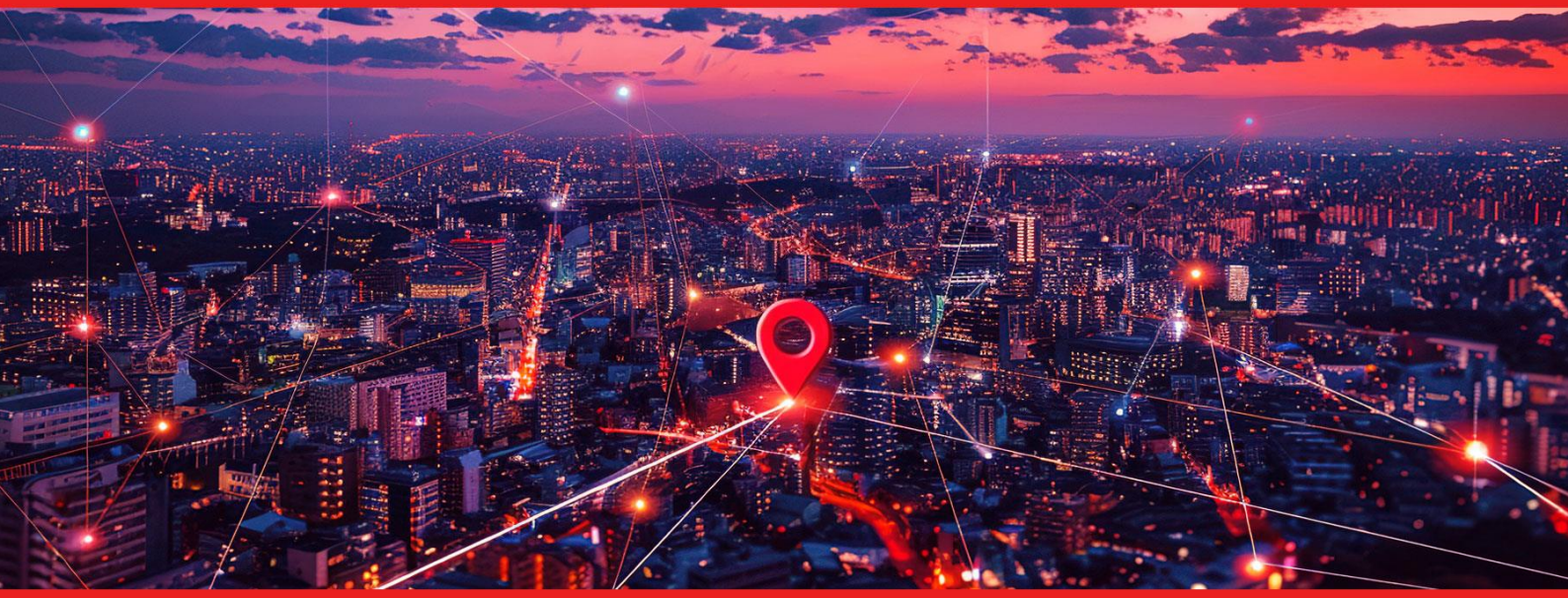
Koris365 Network & Security Patch

Service Description



Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

Copyright

Confidentiality

All information contained in this document is provided as Commercial-in-Confidence. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing. These obligations shall not apply to information which is published or becomes known legitimately and independently of either party.

Contents

Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

1 Summary

1.1 Overview

Network Patch is a managed service that can be added to Network Manage and Monitor to deliver vendor released security patches, updates, IOS upgrades, feature enhancements, and fixes.

1.2 Features

1. Applicable updates for:
    - Core, Distribution, Edge and DC switches
    - WAN routers and devices
    - Wireless LAN controllers
    - Firewalls

2. Varying levels of service available on supported devices:
    - Patch Alert - Proactive alerting of potential critical security vulnerabilities
    - Patch Critical - Includes Patch Alert and remediation of identified vulnerability
    - Patch Yearly - Includes Patch Alert and Patch Critical as well as yearly review, recommendations, and applicable upgrades to relevant devices.
3. Quarterly version reporting

1.3 Suitable Customers

Any organisation with a network infrastructure benefit from Network Patch including:

- Organisations with limited capacity to deliver out of hours maintenance
- Organisations struggling to deploy an effective internal patching solution
- Organisations requiring patching ownership and accountability
- Organisations looking to meet governance requirements by maintaining a security baseline
- Organisations experiencing down-time due to known vulnerabilities of un-patched systems

1.4 Pricing

Network Patch pricing is based on the level of Network Patch purchased and the number and type of devices that require patching.

2 Detailed Service Description

2.1 Pre-requisites

To provide the Network Patch service, Koris365 will require the following:

- Network Manage
- Network Monitor
- The customer must provide a comprehensive list of devices to be patched and a good standard of documentation
- Patching must be up to date before take-on
- Koris365 must be provided with the necessary service accounts and permissions for the systems that require patching
- Network connectivity will be required
- Firewall modifications may be required
- The customer will need to provide at least one named decision maker
- The customer must provide contact details for at least one technical person who will agree maintenance windows
- The customer may be required to provide a technical person on-site to assist with post-patching testing

2.2 Onboarding Procedure

- Koris365 will work with the customer to identify the technical documentation required
- Customer provides Koris365 with technical documentation, including:
    - Any applicable administrative accounts and systems access
    - Network diagrams
    - Configurations
- Koris365 will work with the customer to complete the Unify Onboarding form. The purpose of this document is to collect and support the gathering of necessary information to provision the service, including:
    - Details of customer contacts, escalation paths, and site locations
    - Overview of the customers' environment at point of onboarding
    - Record the collection and the review of the technical documentation
    - High level health check of the customers' environment at point of onboarding
- Koris365 ensures devices and applications to be patched are at a reasonable patch level
- If required customer remediates patch level backlog (Koris365 can provide this service at additional cost)
- Koris365 customer documentation is updated
- Koris365 agrees service schedule with customer
- Business as usual patching commences

2.3 Deliverables

Core Switch	Included
Vulnerability Notification (Patch Alert)	Notification of released vendor critical vulnerabilities
Potential Vulnerability Investigation (Patch Critical)	Identification and investigation of potential high and critical software vulnerabilities
Confirmed Vulnerability Remediation (Patch Critical)	Remediation of identified vulnerability through configuration and or vendor software patch. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Upgrade Review (Patch Yearly)	Annual review of software in operation on supported devices and subsequent recommendations. To include suggested upgrade path.
Yearly Upgrade (Patch Yearly)	Annual installation of vendor recommended software versions. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer

Edge Switch	Included
Vulnerability Notification (Patch Alert)	Notification of released vendor critical vulnerabilities
Potential Vulnerability Investigation (Patch Critical)	Identification and investigation of potential high and critical software vulnerabilities
Confirmed Vulnerability Remediation (Patch Critical)	Remediation of identified vulnerability through configuration and or vendor software patch. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Upgrade Review (Patch Yearly)	Annual review of software in operation on supported devices and subsequent recommendations. To include suggested upgrade path.
Yearly Upgrade (Patch Yearly)	Annual installation of vendor recommended software versions. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer

DC Switch	Included
Vulnerability Notification (Patch Alert)	Notification of released vendor critical vulnerabilities
Potential Vulnerability Investigation (Patch Critical)	Identification and investigation of potential high and critical software vulnerabilities
Confirmed Vulnerability Remediation (Patch Critical)	Remediation of identified vulnerability through configuration and or vendor software patch. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Upgrade Review (Patch Yearly)	Annual review of software in operation on supported devices and subsequent recommendations. To include suggested upgrade path.
Yearly Upgrade (Patch Yearly)	Annual installation of vendor recommended software versions. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer

WAN	Included
Vulnerability Notification (Patch Alert)	Notification of released vendor critical vulnerabilities
Potential Vulnerability Investigation (Patch Critical)	Identification and investigation of potential high and critical software vulnerabilities
Confirmed Vulnerability Remediation (Patch Critical)	Remediation of identified vulnerability through configuration and or vendor software patch. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Upgrade Review (Patch Yearly)	Annual review of software in operation on supported devices and subsequent recommendations. To include suggested upgrade path.
Yearly Upgrade (Patch Yearly)	Annual installation of vendor recommended software versions. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer

WiFi	Included
Vulnerability Notification (Patch Alert)	Notification of released vendor critical vulnerabilities
Potential Vulnerability Investigation (Patch Critical)	Identification and investigation of potential high and critical software vulnerabilities
Confirmed Vulnerability Remediation (Patch Critical)	Remediation of identified vulnerability through configuration and or vendor software patch. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Upgrade Review (Patch Yearly)	Annual review of software in operation on supported devices and subsequent recommendations. To include suggested upgrade path.
Yearly Upgrade (Patch Yearly)	Annual installation of vendor recommended software versions. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer

Firewalls	Included
Vulnerability Notification (Patch Alert)	Notification of released vendor critical vulnerabilities
Potential Vulnerability Investigation (Patch Critical)	Identification and investigation of potential high and critical software vulnerabilities
Confirmed Vulnerability Remediation (Patch Critical)	Remediation of identified vulnerability through configuration and or vendor software patch. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Upgrade Review (Patch Yearly)	Annual review of software in operation on supported devices and subsequent recommendations. To include suggested upgrade path.
Yearly Upgrade (Patch Yearly)	Annual installation of vendor recommended software versions. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer

2.4 Exclusions

- **Fault resolutions without exception**
- **Customer site visits**
- **Remediation of issues caused by customer or third-party changes**
- **Testing of patches**
- **End of Support and End of Software Maintenance applications and system versions**
- **System builds outside vendor defined standards and not pre-approved by Koris365**
- **Host Operating System updates**
- **Koris365 take no responsibility for the introduction of bugs, loss of service, or the loss of data stored caused by the installation of vendor updates**
- **Unused maintenance windows will not be rolled over**

3 Service Level Agreement (SLA)

3.1 Hours of Service

Service	Mon - Fri	Weekends	Bank holidays
Extended	06:00 - 23:00	Excluded	Excluded

Service hours are based upon GMT/BST time zone

3.2 Response & Restoration Times

Priority Level	Response Time	Target Restoration Time
Priority 1	NA	NA
Priority 2	NA	NA
Priority 3	NA	NA
Priority 4 / Service Requests	Next Business Day	NA

Network Patch is a pro-active service. Tickets are raised as service requests but are instigated by Koris365 rather than the customer. Koris365 will contact the customer in accordance with the agreed schedule to arrange a maintenance window. The customer must respond within a reasonable time frame (48 hours) and permit the maintenance window to occur within the extended hours detailed in section 3.1.

- **Koris365 take no responsibility for failure to patch systems where the customer has been unable to agree a maintenance window**
- **Response time is measured from the customer logging a ticket to the customer being contacted to start investigation**
- **Target restoration time is a specified point in time where Koris365 aim to resolve the Incident or Service Request, this will not necessarily be a permanent fix and may need additional work and planned downtime to resolve completely**
- **One service request ticket will be raised per device or application and will remain on hold for the duration**
- **Koris365 take no responsibility where events outside of our control prevent or interrupt a maintenance window**

3.3 Service Level Measurement

The SLA clock will commence on successful logging of a ticket. Elapsed time is measured from the point the ticket is created to the Response Time. The SLA clock then continues until the Restoration time.

During investigation and troubleshooting of a ticket, the SLA Timer will be paused, i.e. the elapsed time is halted, in the following situations;

- Awaiting information, or actions from the customer where Koris365 cannot reasonably be expected to progress the ticket without this information/action
- If customer contact cannot be made after three consecutive attempts, over at least three working days, a final email containing a closure warning will be sent; if Koris365 still do not receive a response the ticket will be closed
- Awaiting information, or actions from a third party where Koris365 cannot reasonably be expected to progress the ticket without this information/action
- Where the problem is associated with a change to the supported system that has not been implemented by Koris365 (ticket will be closed)
- Where the problem is associated with items outside of the supported system (ticket will be closed)
- Where restoration involves time constraints outside of our control, for example, non-redundant systems, backup system limitations, and site visits
- Priority 3, 4, and service request tickets outside of contracted manned hours

Once the information or action has been received by Koris365, the service timer will be reactivated again.

3.4 Service Desk Key Performance Indicators (KPI)

The Service Desk are committed to meeting response and resolution SLAs with a KPI of 95% or above. The Service Desk aim to achieve a KPI of 90% or above on a target average call wait time of 60 seconds or under.

3.5 Ticket Types

3.5.1 Service Requests (IMACD)

Standard service requests are requests for information, moves, additions, changes and deletions (IMACD). No system is at fault and applications are working as expected. This could also take the form of a request that does impact a user's ability to work such as a password reset, in which case these are generally resolved at first point of contact. Most service requests however do not impact the user's ability to work and therefore should be submitted in advance of being required, normally in written format and, where applicable, a standard template such as a new starter form.

Any more than five individual service requests at the same time, i.e. bulk service requests, will require scheduling.

Where a service request is expected to take more than 1 hour to complete then the request will be reviewed and possibly assigned as a separate project.

3.5.2 Incidents

An incident is defined as any event not part of the standard operation of a service which causes an interruption to, or a reduction in the quality of that service.

All incidents and service requests are recorded in the Koris365 ticketing system with a priority selected from the Priority Level Definition table. The priority determines the order in which the Service Desk work on these tickets.

The Incident Priority Code is derived by assessment of the incident's impact and urgency. The Priority code will be provided at the time of logging or by return email. The Priority Code may be re-assigned when the impact or urgency is deemed to have changed.

3.6 Priority Level Definitions

The priority of an incident is defined by assessing both impact and urgency.

- Urgency is a measure of how quickly the system needs to be restored
- Impact is a measure of the potential damage caused by the incident

3.6.1 Incident Urgency

Category	Description
High	• Damage caused by incident increases rapidly • Work that cannot be completed is highly time sensitive
Medium	• Damage caused by incident increases steadily • Work that cannot be completed is moderately time sensitive
Low	• Damage caused by incident increases marginally • Work that cannot be completed is not time sensitive

3.6.2 Incident Impact

Category	Description
High	• Many employees are affected and not able to do their job • Large financial impact • Damage to reputation of business is likely to be high • Many customers are affected
Medium	• A moderate number of employees are affected and not able to do their job • Low financial impact • Damage to reputation of business is likely to be moderate • A moderate number of customers are affected
Low	• A minimal number of employees are affected • Negligible financial impact • Damage to reputation of business is likely to be minimal • A minimal number of customers are affected

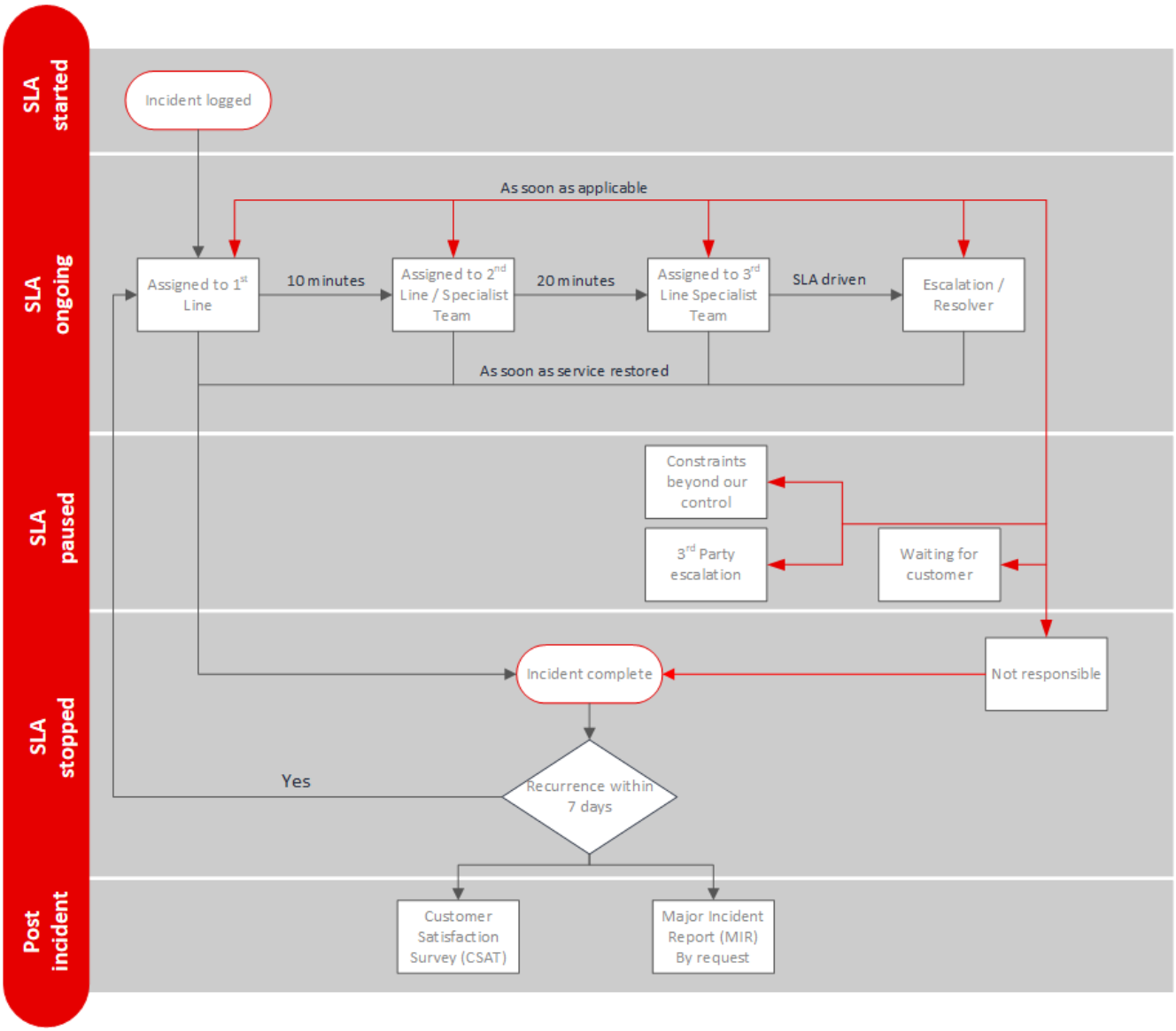
3.6.3 Incident Priority Matrix

		Impact		
		High	Medium	Low
Urgency	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

Priority Level	Action
Priority 1 (P1)	Service Desk provide prioritised, sustained effort using all necessary resources until service is restored
Priority 2 (P2)	Service Desk reprioritise resources from lower priority jobs where necessary to focus on restoring the services
Priority 3 (P3)	Service Desk reprioritise resources from lower priority jobs where necessary
Priority 4 (P4)	Service Desk provide a response using standard operating procedures

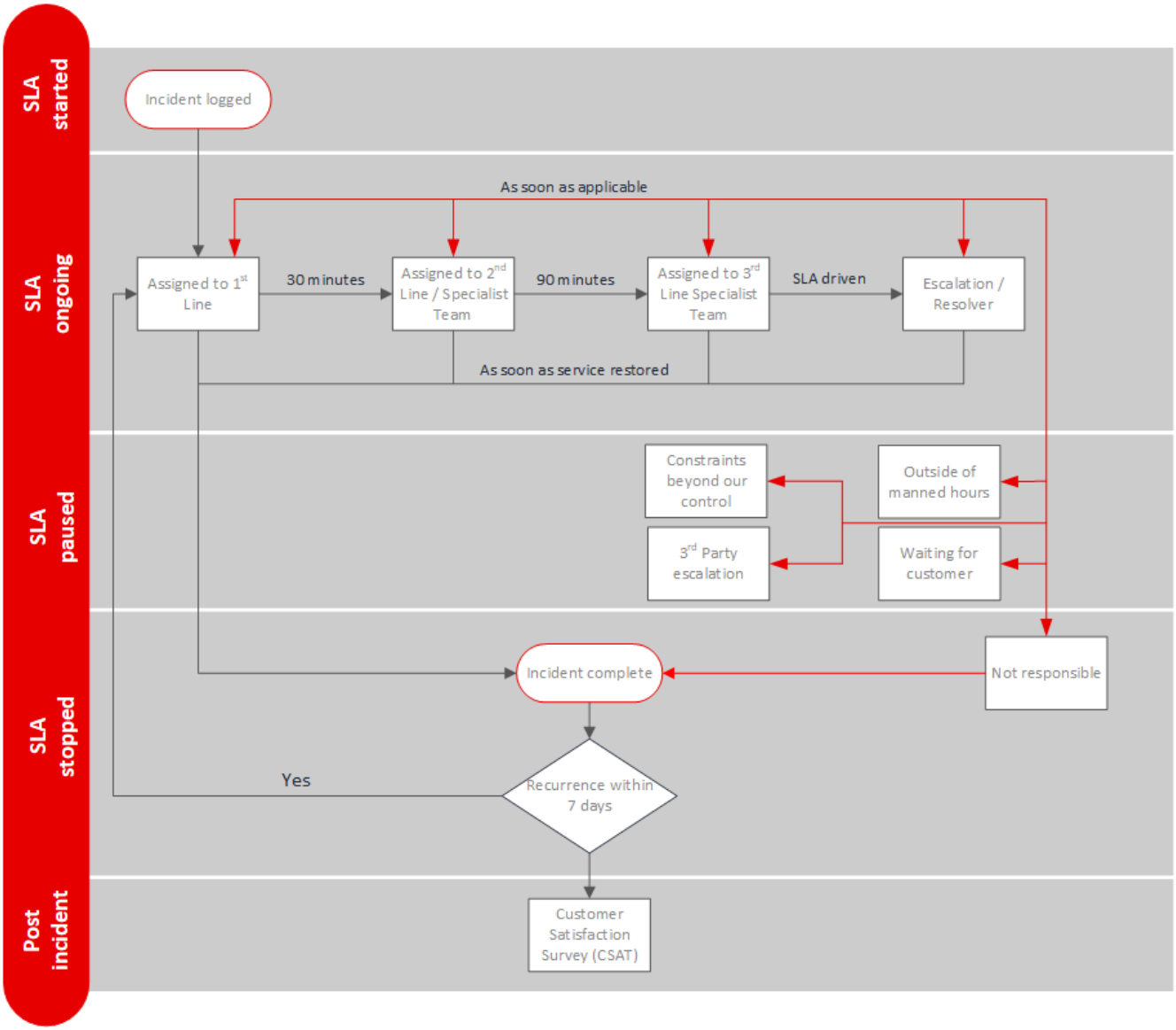
3.7 Ticket Handling and Escalation

3.7.1 P1 and P2 Ticket Flow

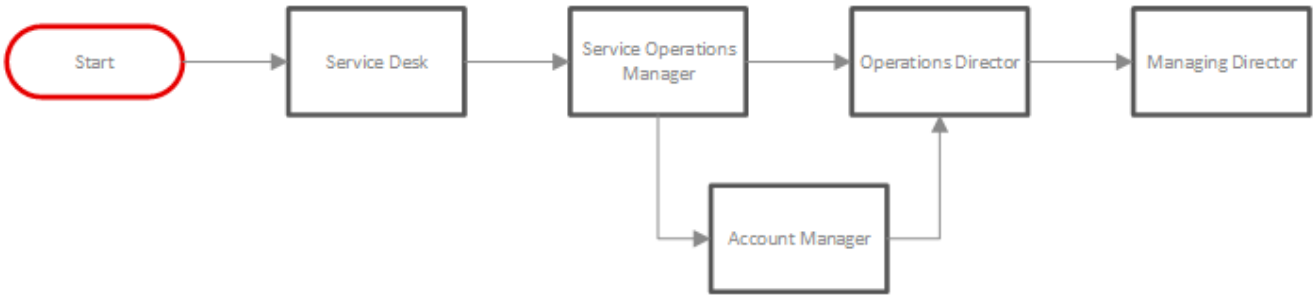


Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

3.7.2 P3 and P4 Ticket Flow



3.7.3 Customer Escalation



4 Offboarding Procedure

On the final day of contract Koris365 will:

- Provide any stored credentials to the customer
- Provide any existing supported systems documentation to the customer
- At the customer's request, engage with the incoming services provider to supply any existing supported systems documentation necessary for transition of the service
- Permanently disable remote access and monitoring
- Cease working on any outstanding tickets and provide an outstanding ticket summary
- Delete customer owned data stored within the Koris365 environment
- Deletion/redaction of customer user records
- Terminate service
-

The customer is expected to:

- Change passwords and disable accounts as necessary for security purposes
- Plan migration of data in advance of termination of service

Koris365 will not:

- Provide details of internal working practices
- Keep a copy of customer owned data stored within the Koris365 environment for future recovery purposes