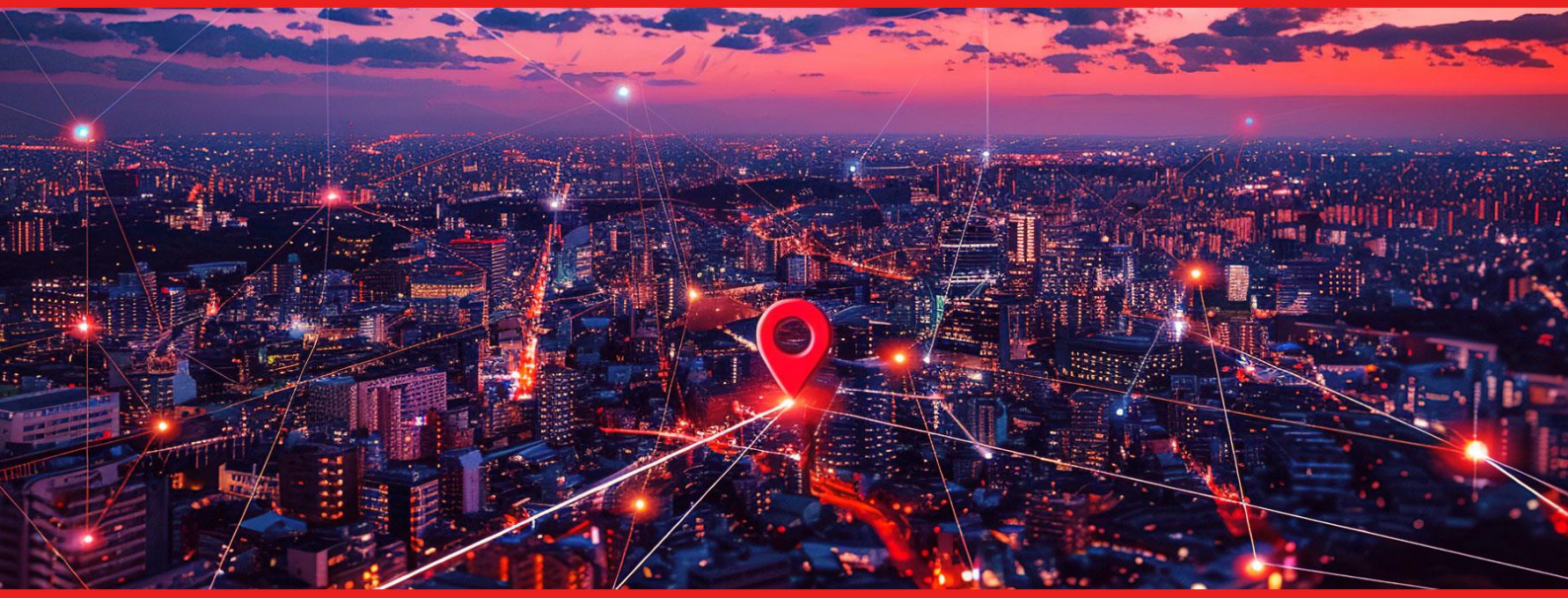
# Koris365 Network & Security Monitor

## 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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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

# 1 Summary

## 1.1 Overview

Network Monitor provides customers with a managed, platform, monitoring and alerting solution. Network Monitor can be delivered as a standalone service or as part of a more comprehensive managed solution.

## 1.2 Features

Network Monitor provides:

Monitoring and alerting for:

- Switches
- WAN services and devices
- Wireless devices
- Firewalls
- Customer dashboard with a standard view
- Monthly exception reporting (customer must also have Network Manage)
- Quarterly lifecycle reporting (customer must also have Network Manage)

## 1.3 Suitable Customers

Any organisation with a network infrastructure can benefit from Network Monitor including:

- Organisations with limited, or no, proactive monitoring capability
- Organisations struggling to deploy an effective internal monitoring solution
- Organisations not getting any value from their existing monitoring solution
- Organisations looking to remove the burden of managing a monitoring solution
- Organisations requiring monitoring ownership and accountability

## 1.4 Pricing

Network Monitor pricing is based on the number and type of devices and interfaces that require monitoring.

# 2 Detailed Service Description

## 2.1 Pre-requisites

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

- The customer must provide a comprehensive list of devices to be monitored complemented with a good standard of documentation
- Koris365 must be provided with the necessary service accounts and permissions for the systems that require monitoring
- Permanent connectivity via a secure VPN L2L tunnel terminated between Koris365 and the customer network
- A route into the Koris365 monitoring platform will need to be configured from within the customer's network
- 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 receive alerts

## 2.2 Onboarding Procedure

1. Koris365 will work with the customer to identify the technical documentation required
2. Customer provides Koris365 with technical documentation, including:
    a. Any applicable administrative accounts and systems access
    b. Network diagrams
    c. Configurations
3. Koris365 will work with the customer to complete the Unify Services Onboarding form. The purpose of this document is to collect and support the gathering of necessary information to provision the service, including:
    a. Details of customer contacts, escalation paths, and site locations
    b. Overview of the customers' environment at point of onboarding
    c. Record the collection and the review of the technical documentation
    d. High level health check of the customers' environment at point of onboarding
4. Koris365 Consultants make initial deployment
5. Koris365 compares initial deployment with documentation and if required liaises with customer to perform fine tuning
6. If there are discrepancies between the initial deployment and customer provided technical documentation, then remediation will be required and chargeable
7. Koris365 customer documentation is updated
8. Koris365 completes final deployment
9. Alert notifications and applicable portal access created
10. Reporting templates designed and agreed in accordance with customer requirements.
11. Business as usual monitoring and alerting commences

## 2.3 Deliverables

| Core Switch | Included |
|---|---|
| Monitoring | Monitoring and notification for:<br>• Node up/down, reload, interface down, packet loss, backup failure, environmental (PSU's, fans, sensors)<br>• CPU, memory, and disk utilisation<br>• Interface utilisation<br>• Switchport utilisation<br>• Stack failures |
| Device Backup (customer must also have Network Manage) | Daily configuration backups and storage |
| Threshold changes | Ongoing maintenance of monitoring thresholds |

| Edge Switch | Included |
|---|---|
| Monitoring | Monitoring and notification for:<br>• Node up/down, reload, interface down, packet loss, backup failure, environmental (PSU's, fans, sensors)<br>• CPU, memory, and disk utilisation<br>• Interface utilisation<br>• Switchport utilisation<br>• Stack failures |
| Device Backup (customer must also have Network Manage) | Daily configuration backups and storage |
| Threshold changes | Ongoing maintenance of monitoring thresholds |

| Data Centre Switch | Included |
|---|---|
| Monitoring | Monitoring and notification for:<br>• Node up/down, reload, interface down, packet loss, backup failure, environmental (PSU's, fans, sensors)<br>• CPU, memory, and disk utilisation<br>• Interface utilisation<br>• Switchport utilisation<br>• Stack failures |
| Device Backup (customer must also have Network Manage) | Daily configuration backups and storage |
| Threshold changes | Ongoing maintenance of monitoring thresholds |

| WAN | Included |
|---|---|
| Monitoring | Monitoring and notification for:<br>• Node up/down, reload, interface down, packet loss, backup failure, environmental (PSU's, fans, sensors)<br>• CPU, memory, and disk utilisation<br>• Interface utilisation<br>• Switchport utilisation<br>• Stack failures |
| Device Backup (customer must also have Network Manage) | Daily configuration backups and storage |
| Threshold changes | Ongoing maintenance of monitoring thresholds |

| WiFi | Included |
|---|---|
| Monitoring | Monitoring and notification for:<br>• Node up/down, reload, interface down, packet loss, backup failure, environmental (PSU's, fans, sensors)<br>• CPU, memory, and disk utilisation<br>• Interface utilisation<br>• AP registration<br>• Number of client associations |
| Device Backup (customer must also have Network Manage) | Daily configuration backups and storage |
| Threshold changes | Ongoing maintenance of monitoring thresholds |

| Firewall | Included |
|---|---|
| Monitoring | Monitoring and notification for:<br>• Node up/down, reload, interface down, packet loss, backup failure, environmental (PSU's, fans, sensors)<br>• CPU, memory, and disk utilisation<br>• Interface utilisation<br>• L2L VPN down |
| Device Backup (customer must also have Network Manage) | Daily configuration backups and storage |
| Threshold changes | Ongoing maintenance of monitoring thresholds |

| Reporting | Included |
|---|---|
| Exception Report (customer must also have Network Manage) | Monthly reporting of:<br>Major Incidents, security notifications, backup and inventory validation, license utilisation, average snapshot of CPU, memory, and interface utilisation, switchport usage |
| Lifecycle Report (customer must also have Network Manage) | Quarterly reporting of:<br>Device end-of-life status in a red, amber, green format |

## 2.4 Exclusions

- **Fault resolutions without exception**
- **Customer site visits**
- **Remediation of issues caused by customer or third-party changes**
- **Although performance/resource threshold monitoring is included and may allow customers to proactively prevent an outage, sudden unpredictable outages may still occur**
- **Development of monitoring and management features**
- **This is not a security monitoring or Security Information and Event Management (SIEM) service**
- **Service wide outages that are beyond our control such as Internet Service Provider (ISP) failures will generate alerts but will also prevent polling, resulting in any coinciding issues becoming undetectable for the duration of the outage**
- **Renotification of repeat failures where the customer has not carried out remediation or recommendations**
- **Customer dashboard customisation**
- **Switchport usage monitoring if not explicitly included**

# 3 Service Level Agreement (SLA)

## 3.1 Hours of Service

| Service | Mon - Fri | Weekends | Bank holidays |
|---|---|---|---|
| 24/7 | Monitoring and alerting is automated and running 24/7.<br>08:00 – 18:00 for monitoring alterations or platform help | Monitoring and alerting is automated and running 24/7. | Monitoring and alerting is automated and running 24/7. |

**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 | 48 hours |

**Network Monitor is primarily an automated service. Tickets pertaining specifically to this service will be low priority and treated as a Priority 4 / Service Request. Tickets will usually be requests to alter monitoring thresholds or to add and remove devices. If other Koris365 Managed Services that include remediation have been purchased, then tickets resulting from Network Monitor alerts will be treated under the SLA terms for that service.**

- **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**
- **Restoration may take longer than target time due to circumstances outside of our control, for example, non-redundant systems, backup system limitations, site visits, third party SLAs and patching cycles**
- **Incidents may be resolved by the service desk, or a third party**
- **Target restoration times are based upon contracted hours.**

## 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 Classification

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<br>• Work that cannot be completed is highly time sensitive |
| Medium | • Damage caused by incident increases steadily<br>• Work that cannot be completed is moderately time sensitive |
| Low | • Damage caused by incident increases marginally<br>• 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<br>• Large financial impact<br>• Damage to reputation of business is likely to be high<br>• Many customers are affected |
| Medium | • A moderate number of employees are affected and not able to do their job<br>• Low financial impact<br>• Damage to reputation of business is likely to be moderate<br>• A moderate number of customers are affected |
| Low | • A minimal number of employees are affected<br>• Negligible financial impact<br>• Damage to reputation of business is likely to be minimal<br>• A minimal number of customers are affected |

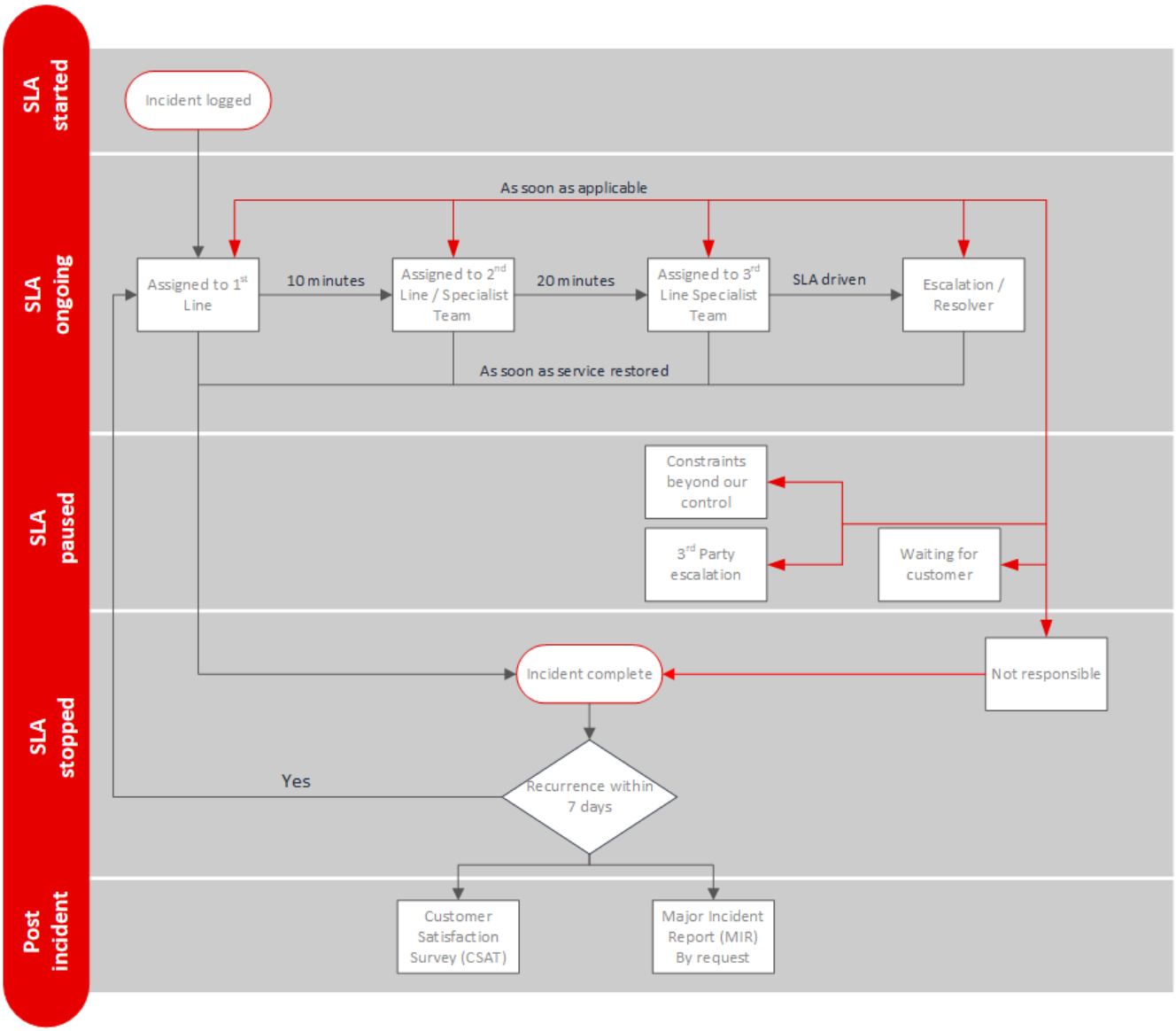
## 3.6.3 Incident Priority Matrix

| | | 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 & Escalation

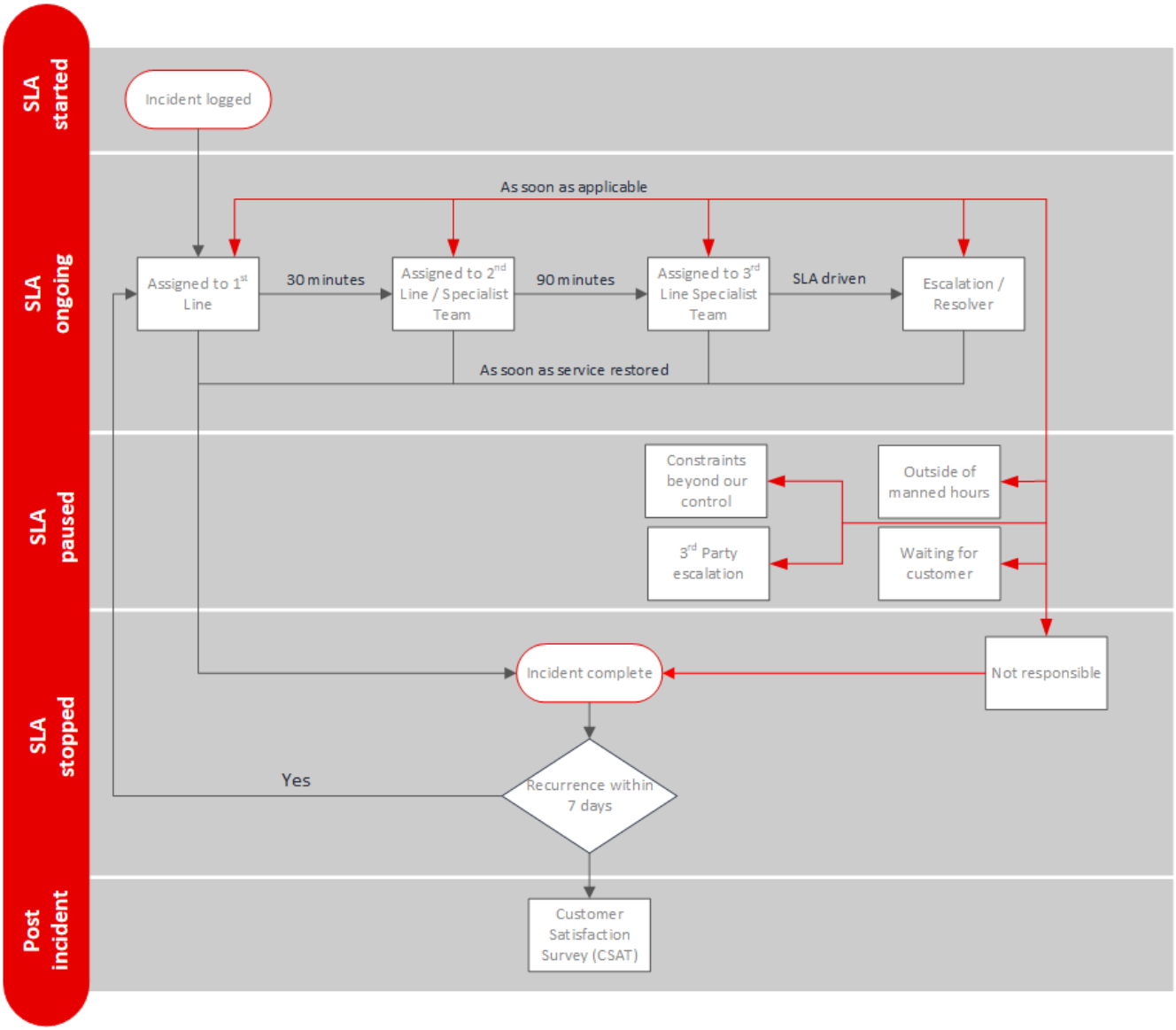
### 3.7.1 P1 and P2 Ticket Flow



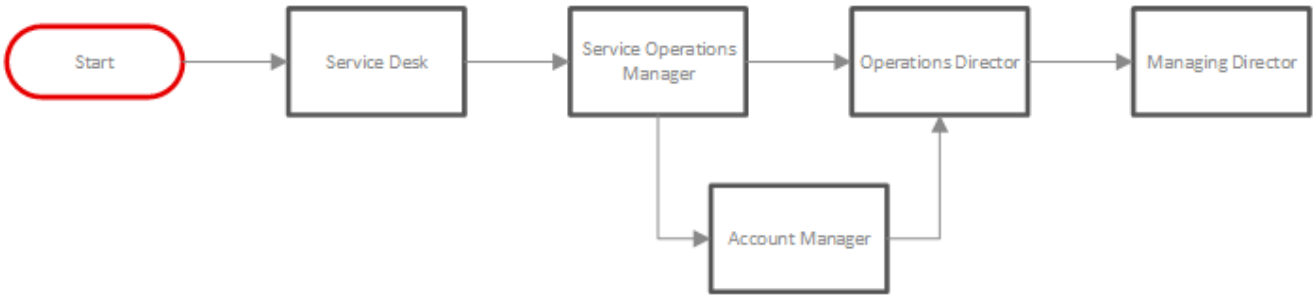



Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

## 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