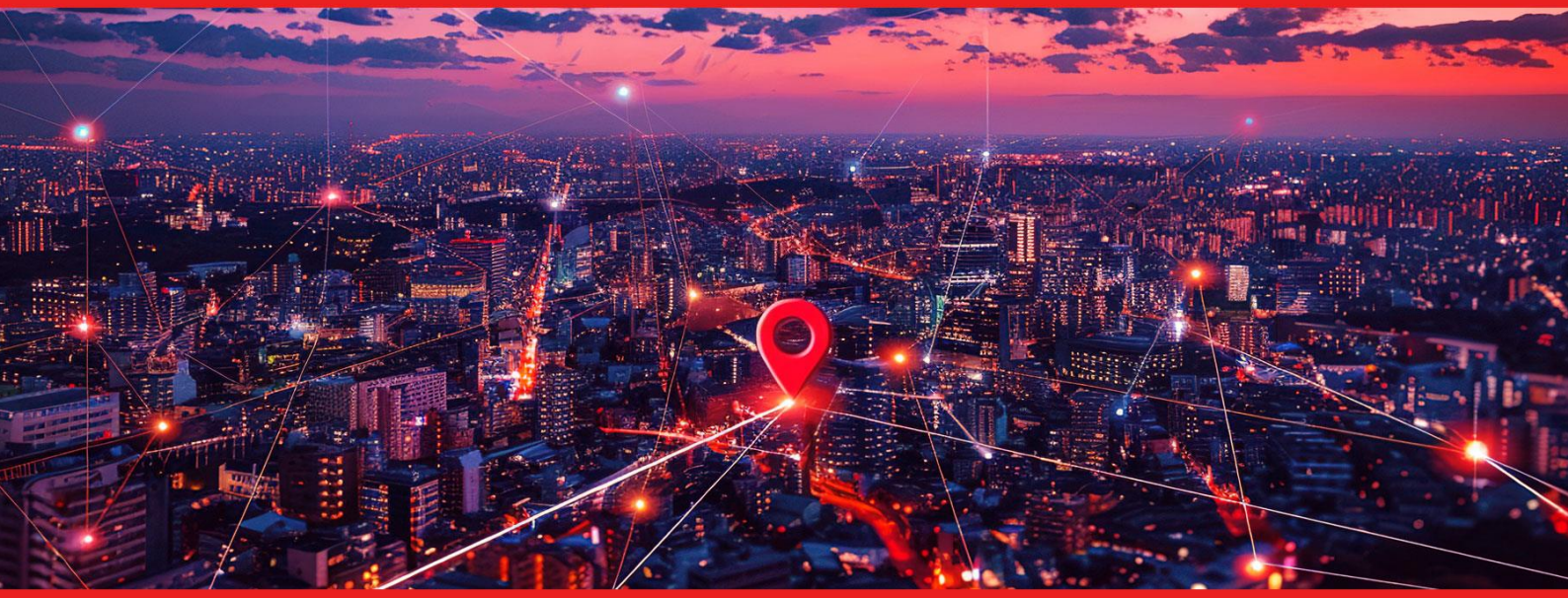
Koris365 Network & Security Resolve

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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

Network Resolve provides a technical escalation point for a customer's IT department to aid in the troubleshooting and resolution of problems across the network infrastructure. Network Resolve can also be combined with other Unify services to form part of a more comprehensive managed solution.

1.2 Features

Network Resolve provides:

- Resolving issues arising in a customers' network infrastructure including:
  - Core, Distribution, and edge switching
  - DC Switching – Fabric, Leaf and Spine, or one-tier flat mesh architectures
  - Wide Area Network
  - WiFi
  - Firewalls
  - Identity management
  - SD-WAN
  - Software Defined Networking
- Liaising with third-party vendors for incidents related to contracted hardware and software
- Problem management
- 3rd party circuit management

1.3 Suitable Customers

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

- Organisations with limited, or no inhouse IT resource
- Organisations looking for peace of mind that the expertise to deal with complex IT issues is available
- Organisations looking to deploy new solutions without the need to retrain
- Organisations looking to expand without the burden of IT recruitment

1.4 Pricing

Network Resolve pricing is based on the number and type of devices, services, and sites.

2 Detailed Service Description

2.1 Pre-requisites

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

- The customer must provide a comprehensive list of devices to be supported and a good standard of documentation
- The supported system must be in a good operational state, with best-practice configuration and good vendor support status
- The customer must have out of band management cards configured (e.g. CIMC)
- The customer must provide relevant company detail such as quantity of users, locations, hours of work
- The customer must be prepared to facilitate remote access and provide credentials as necessary during support
- The customer will need to provide at least one named decision maker
- The customer must specify at least one person who is able to raise tickets (typically limited to IT personnel)
- The customer must provide a list of at least one technical person who can assist or take ownership when an issue, or part of, is out of scope

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. A full audit of the Customer's Network infrastructure may be compulsory depending on the level of information available. The audit is not included in Network Resolve and will be an additional cost to the Customer.
4. 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
5. If required, Koris365 make recommendations to remedy any pre-existing faults or misconfigurations
6. If applicable, customer remediates any pre-existing faults or misconfigurations (Koris365 can provide professional services resource at additional cost if required)
7. Koris365 customer documentation is updated
8. Customer receives welcome pack including ticket logging instructions
9. Business as usual service commences

2.3 Deliverables

Core Switch	Included
Switching performance faults	Diagnosing performance issues such as: Interface drops, errors, throughput, utilisation, CPU and memory.
Access faults	Investigating issues relating to layer 2 switching and services such as: DHCP, access VLANs, Voice VLANs, and port issues.
Routing services faults	Diagnosing issues relating to routing services such as: Dynamic, static, policy-based routing, and first hop redundancy protocols. Working on associated issues with 3rd parties such as ISP's
Security issues	Troubleshooting security and associated issues such as: NAC, policy-based security (ACL's), port security and 802.1x port-based authentication
Switch connectivity faults	Investigating faults relating to multiple switch connectivity such as: Virtual switching, stacking, 802.1q trunking, VTP and aggregated channels (LACP, PAgP)
Traffic control faults	Troubleshooting performance and configuration issues such as: STP, broadcasts, network loops, storm control, QoS classification, markings and policies
Environmental/Hardware faults	Investigating physical and environmental related faults such as: Faulty PSU's, fans, chassis, cabling and optics.
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.

Edge Switch	Included
Switching performance faults	Diagnosing performance issues such as: Interface drops, errors, throughput, utilisation, CPU and memory.
Access faults	Investigating issues relating to layer 2 switching and services such as: DHCP, access VLANs, Voice VLANs, and port issues.
Security issues	Troubleshooting security and associated issues such as: NAC, policy-based security (ACL's), port security and 802.1x port-based authentication
Switch connectivity faults	Investigating faults relating to multiple switch connectivity such as: Virtual switching, stacking, 802.1q trunking, VTP and aggregated channels (LACP, PAgP)
Traffic control faults	Troubleshooting performance and configuration issues such as: STP, broadcasts, network loops and storm control, QoS classification, markings and policies
Environmental/Hardware faults	Investigating physical and environmental related faults such as: Faulty PSU's, fans, chassis, cabling and optics.
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.

DC Switch	Included
Switching performance faults	Diagnosing performance issues such as: Interface drops, errors, throughput, utilisation, CPU and memory.
Access faults	Investigating issues relating to layer 2 switching and services such as: DHCP, access VLANs, Voice VLANs, and port issues.
Security issues	Troubleshooting security and associated issues such as: NAC, policy-based security (ACL's), port security and 802.1x port-based authentication
Switch connectivity faults	Investigating faults relating to multiple switch connectivity such as: Virtual switching, stacking, 802.1q trunking, VTP and aggregated channels (LACP, PAgP)
Traffic control faults	Troubleshooting performance and configuration issues such as:

	STP, broadcasts, network loops and storm control, QoS classification, markings and policies
Environmental/Hardware faults	Investigating physical and environmental related faults such as: Faulty PSU's, fans, chassis, cabling and optics.
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.

WAN	Included
Routing faults	Investigating connectivity issues relating to static, dynamic and policy-based routing across technologies such as: IPSec VPN's, SD-WAN, MPLS, VPLS and point-to-point connectivity.
Traffic control faults	Investigating issues relating to network reliability, security, performance, and bandwidth such as: Bottlenecks, packet drops on policy maps and interfaces, traffic shaping and working with providers to identify QoS service plane problems.
Media faults	Diagnosing issues caused by physical layer problems such as: Cabling, optics, and provider equipment.
Environmental/Hardware	Investigating physical and environmental related faults on supported devices such as: Faulty PSU's, fans, sensors, and chassis.
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.

WiFi	Included
WLAN faults	Diagnosing WLAN issues such as: Client associations, AP joining, wireless coverage, roaming, interference, and performance.
WLC faults	Investigating faults relating to wireless controllers such as: access, redundancy, DHCP and mobility issues
Security faults	Troubleshooting security and authentication related issues such as: Radius, LDAP, TACACS, webauth bundle, MAC filtering and access control lists.
Environmental/Hardware	Investigating physical and environmental related faults such as: Faulty PSU's, fans, sensors and chassis.
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.

Firewalls	Included
Access control faults	Diagnosing access control type related issues such as: Access policies, application inspection, QoS, TCP/UDP connections and NAT
Failover faults	Troubleshooting issues relating to high availability firewalls and related functionality such as: Synchronisation, peer connectivity, missed heartbeats and error states.
VPN faults	Investigating issues relating to IPsec and SSL VPN's such as: VPN client issues, site to site VPN's, transform sets, SSL-VPN Portal access, routing, access and policies.
Network faults	Troubleshooting issues relating network connectivity such as: Static routing, Dynamic routing, DHCP and SD-WAN.
Application control faults	Troubleshooting issues relating to Application layer services such as: Intrusion Prevention System, Antivirus, Web filter, advanced malware protection, DNS Filter, Web Application Firewall, Endpoint control, Anti-spam filter and AntiDDos Protection
Firewall Management and Log Applications	Investigating issues relating to firewall management and logging applications such as: FMC, WMS, Fortimanager, ASDM, Fortianalyser and Dimensions.

Environmental/Hardware faults	Investigating physical and environmental related faults such as: Faulty PSU's, fans, chassis, cabling and optics.
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.
Additional Functions/Modules	Diagnosing issues related to additional inbuilt services such as: Wireless controllers and security fabrics.

Identity / Network Management	Included
Access control faults	Investigating faults relating to networks access control for devices and users based on the configured authentication and authorisation policies.
System level faults	Investigating system performance and integration issues such as: Server resource, application integration, 3rd party authentication servers and protocols, LDAP, Radius, TACACS and MFA
Environmental/Hardware faults	
OS faults	Investigating and identification of OS related issues such as: OS bugs, vulnerabilities, field notices, interoperability, and features.

2.4 Exclusions

- Remediating pre-existing issues
- System administration
- Any service outside of fault resolution
- Replacement parts or the addition of new hardware
- Configuration and operational issues with any 3rd party applications or hardware
- Liaising with third-party vendors for incidents related to hardware and software outside of the supported system
- Performance issues or failures caused by underspecified hardware resources
- Software versions categorised as deferred by the vendor, will only be progressed on a reasonable efforts basis
- Remediating issues caused by customer or third-party changes
- Issues arising directly or indirectly from the addition of new sites not pre-approved by Koris365
- Any issues caused by connected equipment, integrations, and infrastructure not supported and where the supported equipment is ruled out as being at fault.
- Koris365 take no responsibility for failure of hardware or the loss of data stored
- Seeding of new backup, backup copy, and replica jobs, or the provision of any temporary storage required
- Koris365 take no responsibility for the failure of magnetic tapes, UPS batteries, RAID cache batteries, or similar consumables resulting in a loss of data
- Training
- Issues caused by the improper management of security certificates
- Support for end user, client devices, and third-party internet connections
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Any activity that requires a site visit
- Troubleshooting of bespoke applications, bespoke alterations, or third-party integrations
- Troubleshooting configurations that are not supported by the vendor or do not follow vendor best practice
- End of life operating systems, applications, and devices
- OS patching, migrations or upgrades
- Koris365 will not implement changes that carry a high risk of organisation disruption without suitable contingency
- Limitations may apply to third-party vendors
- Resolving issues with systems that are beyond economical repair e.g. the system would take longer to repair than to restore or rebuild
- Diagnosis of hardware faults of systems without appropriate vendor tools installed

3 Service Level Agreement (SLA)

3.1 Hours of Service

Service	Mon - Fri	Weekends	Bank holidays
Standard	08:00 – 18:00 Standard Hours	Excluded	Excluded
24/7	08:00 – 18:00 Standard Operation (P1-P4) 18:00 – 08:00 Out of Hours (P1 and P2 incidents only)	Included (P1 and P2 incidents only)	Included (P1 and P2 incidents only)

Service hours are based upon GMT/BST time zone

3.2 Response & Restoration Times

Priority Level	Response Time	Target Restoration Time
Priority 1	30 minutes	4 hours
Priority 2	1 hour	8 hours
Priority 3	1 hour	32 hours
Priority 4 / Service Requests	Next Business Day	48 hours

Network Resolve tickets will always be treated as incidents. Service requests are not included in Network Resolve, but available as part of Network Manage.

- **Priority 1 and 2 tickets must be raised or followed up via a phone call to the service desk**
- **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, an on-site engineering support team, or a third party**
- **Where the incident is determined to be the responsibility of a third party Koris365 will ensure all incident details are passed to the third party without undue delay**
- **Target restoration times are based upon contracted hours. Tickets not classed as Priority 1 and 2 will not be worked on outside of manned 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 and 4 tickets outside of contracted manned hours

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

Priority 1 and 2 calls will be measured throughout the 24/7 period where a 24/7 contract has been purchased.

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 • 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

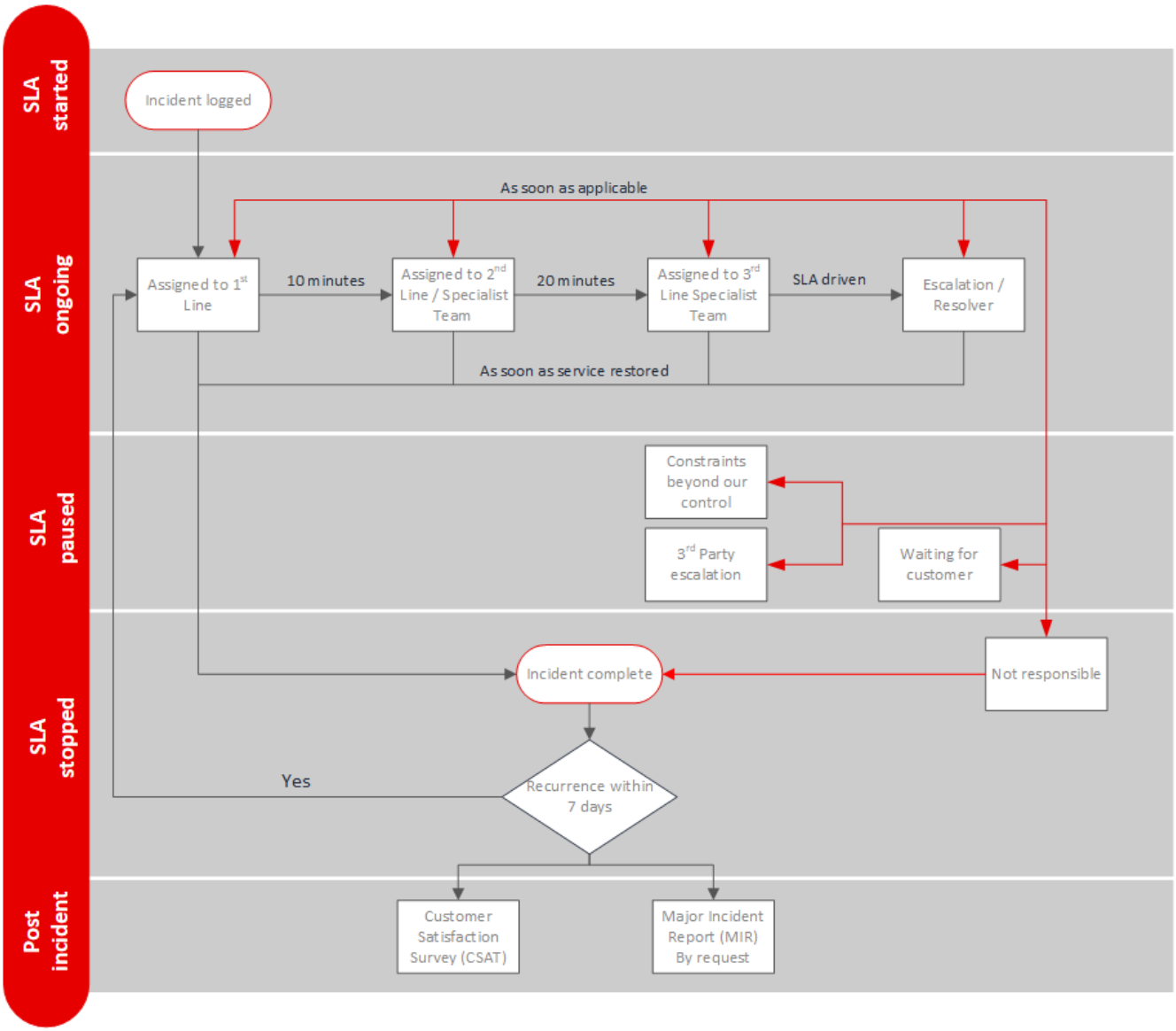
3.6.3 Incident Priority Matrix

		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

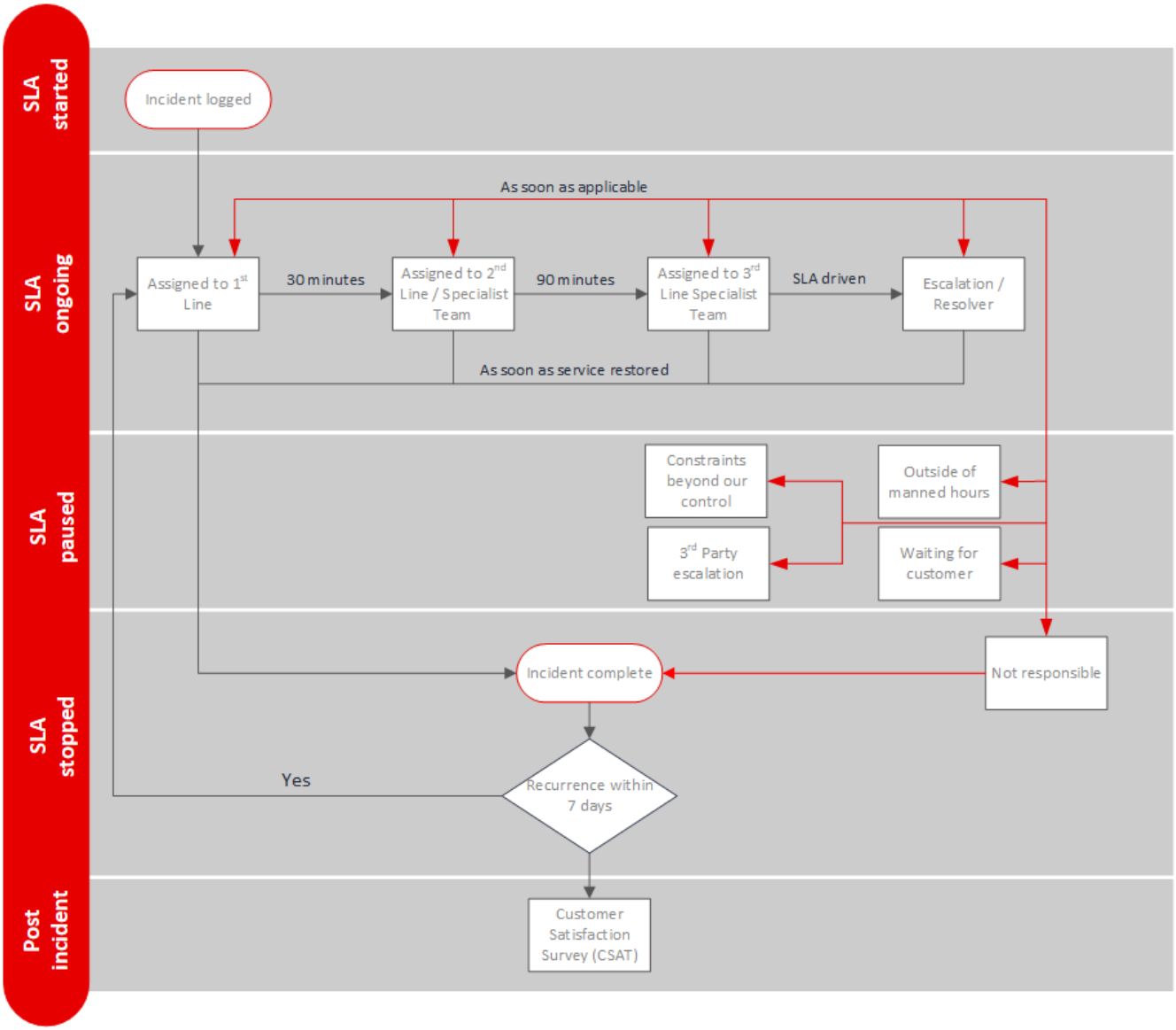
3.7 Ticket Handling and Escalation

3.7.1 P1 and P2 Ticket Flow

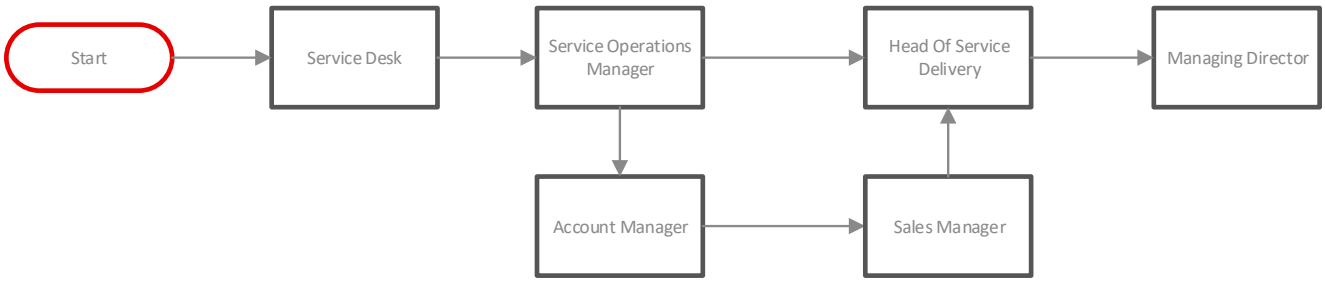


Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

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