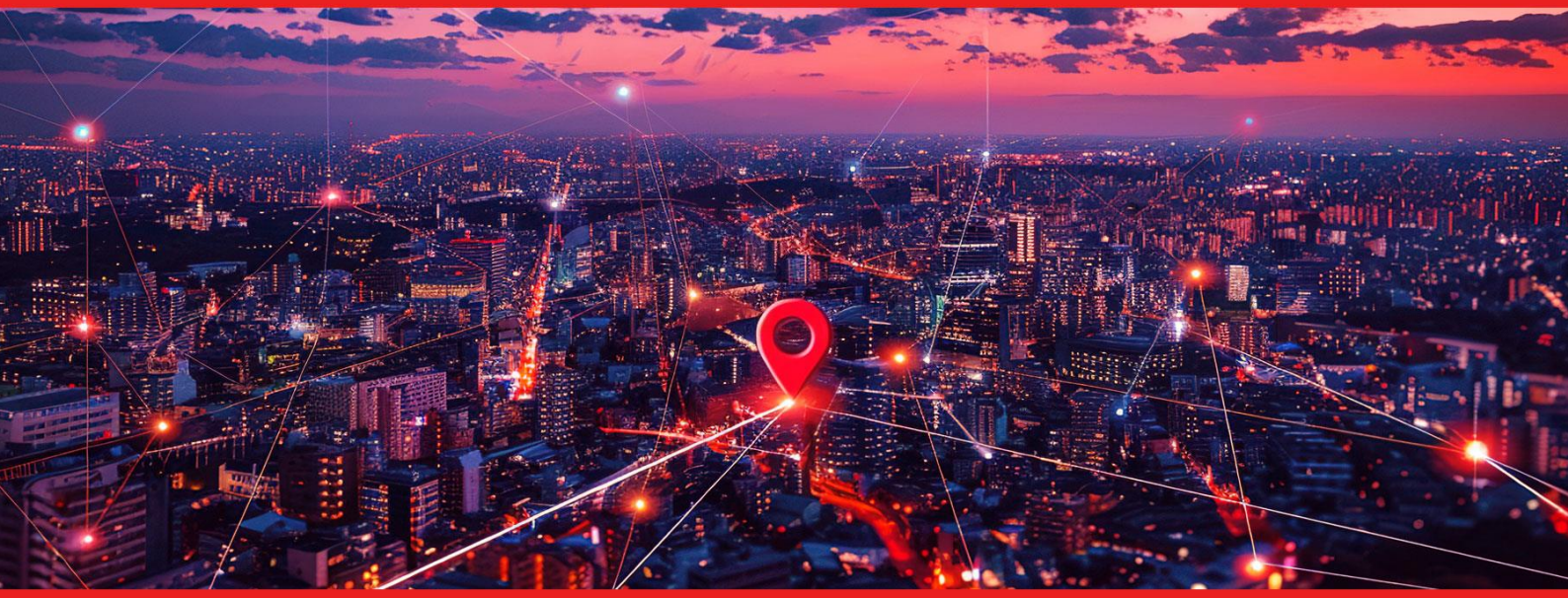
Koris365 Network & Security Manage

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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 Manage provides customers with the day-to-day systems administration of their Networking infrastructure such as changes to security, access, and routing policies along with general routine configuration changes. Network Manage is not a standalone service, its purpose is to form a comprehensive managed solution when combined with Network Resolve.

1.2 Features

Network Manage provides:

- Management of Networking infrastructure including:
  - Core, DC, and edge switching
  - Wide Area Network
  - WiFi
  - Firewalls
  - Identity / Network Management
  - SD-WAN
  - Software Defined Networking
- Management of backups including:
  - Core Switches
  - Edge Switches
  - Data Centre Switches
  - Routers
  - Wireless LAN Controllers
  - Firewalls
- Monthly service reporting
- Monthly exception reporting (customer must also have Network Monitor)
- Quarterly lifecycle reporting (customer must also have Network Monitor)

1.3 Suitable Customers

Any organisation with a Network infrastructure can benefit from Network Manage including:

- Organisations with limited, or no inhouse IT resource
- Organisations struggling to manage complex IT infrastructures
- Organisations looking for more support and guidance towards their IT roadmap
- Organisations not getting value from their existing management solution
- Organisations looking to remove the day-to-day burden of routine administrative tasks
- Organisations requiring management ownership and accountability

1.4 Pricing

Network Manage pricing is based on the number and type of devices and services to be managed.

2 Detailed Service Description

2.1 Pre-requisites

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

- Network Resolve
- The customer must provide a comprehensive list of devices to be managed complemented with 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 provide permanent remote access
- Koris365 must be provided with administrative accounts for the systems to be managed
- 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)

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 Networking 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 and customer agree on IT procedures e.g. new starters, leavers, permission changes
8. Koris365 customer documentation is updated
9. Customer receives welcome pack including ticket logging instructions
10. Business as usual service commences

2.3 Deliverables

Core Switch	Included
General Switch Management	Configuration of: Switch management, virtual switching, access policy, NTP, AAA, VTY, SNMP
Interface Management	Configuration or addition of: Access interfaces, trunk interfaces, aggregated channels, layer 3 VLAN's, port security, SD Access
Traffic Control Management	Configuration or addition of: VLAN's, SPAN, Mirroring, QoS, STP, storm control
Routing Services Management	Configuration or addition of: Dynamic routing, static routes, FHRP, policy-based routing.
Security Management	Configuration or addition of: Access control lists, NAC, 802.1x, SD Access
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

Edge Switch	Included
General Switch Management	Configuration of: Switch management, virtual switching, access policy, NTP, AAA, VTY, SNMP
Interface Management	Configuration or addition of: Access interfaces, trunk interfaces, aggregated channels, layer 3 VLAN's, port security, SD Access
Traffic Control Management	Configuration or addition of: VLAN's, SPAN, Mirroring, QoS, STP, storm control
Security Management	Configuration or addition of: Access control lists, NAC, 802.1x, SD Access
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

DC Switch	Included
General Switch Management	Configuration of: Switch management, virtual switching, access policy, NTP, AAA, VTY, SNMP
Interface Management	Configuration or addition of: Access interfaces, trunk interfaces, aggregated channels, layer 3 VLAN's, port security, SD Access
Traffic Control Management	Configuration or addition of: VLAN's, SPAN, Mirroring, QoS, STP, storm control
Security Management	Configuration or addition of: Access control lists, NAC, 802.1x, SD Access
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

WAN	Included
Routing Services Management	Configuration or addition of: Dynamic routing and protocols, static routes, layer 3 interfaces, policy-based routing, next hop resolution protocols, SD-WAN
Traffic control management	Configuration or addition of: Access control lists, QoS, class maps, policy maps, SD-WAN
Service Provider management	Authority with WAN provider to request minor routing and network changes such as advertising additional networks
General Device management	Configuration or addition of: General configuration items such as access policy, DHCP, AAA and NTP
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

WiFi	Included
WLAN Management	Configuration or addition of: WLANs including advanced settings, QoS, RF management, AP management
General WLC Management	Configuration or addition of: WLC access, NTP, Radius authentication, LDAP synchronization, SNMP, syslog, logging configuration
Security Management	Configuration or addition of: Radius, Webauth bundle, LDAP, TACACS, MAC filtering, access control lists, guest access, SD-Access
Network Configuration Management	Configuration or addition of: Network connectivity, DHCP, Interfaces, VLAN, SD-Access
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

Firewalls	Included
Access Control Management	Configuration or addition of: Access policies, access control lists, Objects, NAT
General Firewall Management	Configuration or addition of: Firewall access, NTP, AAA, Radius, LDAP, SNMP, Syslog
VPN Configuration Management	Configuration or addition of: Transform sets, IPsec profiles, SSL profiles, clientless VPN, site to site VPN, remote access VPN, group policies, split tunnelling, access control
Network configuration management	Configuration or addition of: Static and dynamic routing, DHCP, Interface, VLAN's, SD-WAN
Application Control Management	Configuration of: Intrusion Prevention, antivirus, web filter, advanced malware, DNS Filter, web application firewall, endpoint control, anti-spam filter
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

Identity Services / Network Management	Included
Access Control Management	Configuration or addition of: Device profiles, authorisation profiles, authentication settings, conditions, results, policies, SD-Access
General Management	Configuration or addition of: User / Administrator access, NTP, Radius, LDAP, SNMP, Syslog, logging
License Management	Smart licensing, applying licenses
Backup Management (Must include Unify Monitor)	Daily configuration backups

Reporting	Included
Service Report	Monthly reporting of: Ticket analysis, SLA compliance, client survey results
Exception Report (Must include Unify Monitor)	Monthly reporting of: Major Incidents, security notifications, backup and replication validation, license utilisation, average snapshot of CPU, memory, and interface utilisation
Lifecycle Report (Must include Unify Monitor)	Quarterly reporting of: Device end-of-life status in a red, amber, green format

2.4 Exclusions

- **Remediation**
- **Koris365 will investigate license requirements during any installations and will make recommendations but are not responsible for compliance, Software Asset Management, or the provision of licenses**
- **This is not Backup as a Service (BaaS). Koris365 will advise on suitable backup infrastructure but it is the responsibility of the customer to invest appropriately in a solution that meets organisation Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), archiving, and resilience objectives**
- **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 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**
- **Disaster recovery planning and testing**
- **Deployment of any previously unconfigured sites, services, features, new infrastructure, or applications**
- **Training**
- **Development**
- **Certificate management and installation**

- Direct end user service requests (tickets must be raised by named representative who can authorise and provide the necessary information to fulfil the request)
- This is not a security service
- This is not a compliance service. It is the responsibility of the customer to provide Koris365 with validated information adhering to company compliance policies.
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Any activity that requires a site visit
- Management of bespoke applications, bespoke alterations, or third-party integrations
- Configurations that are not supported by the vendor or do not follow vendor best practice
- End of life operating systems, applications, and devices
- Patching, major version 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
- The provision of additional resources such as CPU, memory, disk, and IP addresses where sufficient spare capacity does not exist2
- Any request likely to exceed 1 hour

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

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 Manage tickets will predominantly be treated as a Service Request. A ticket may be treated as an incident if Koris365 are performing a task to prevent an imminent outage.

- 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 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, 4, and service request tickets received 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

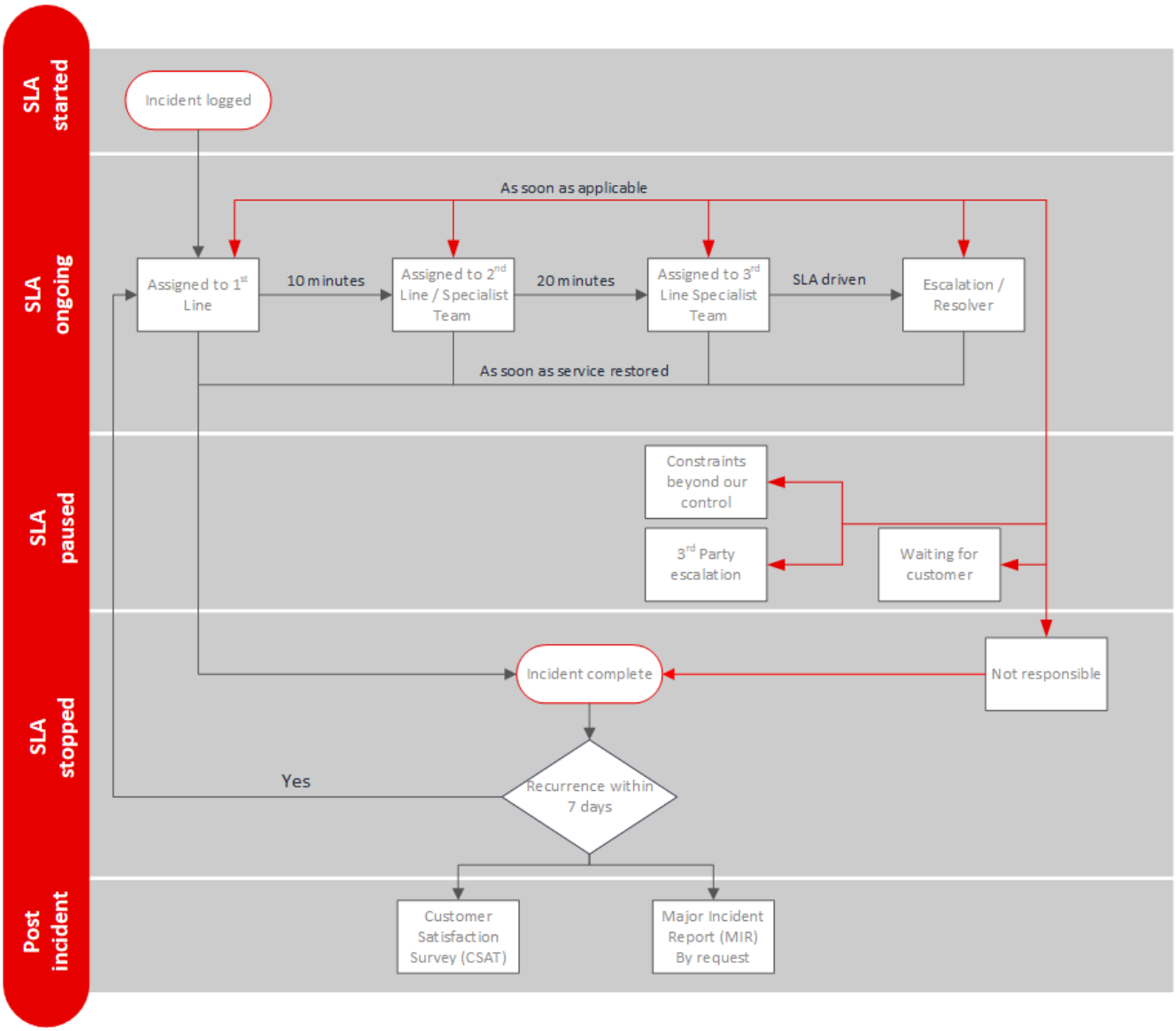
3.6.3 Incident Priority Matrix

		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

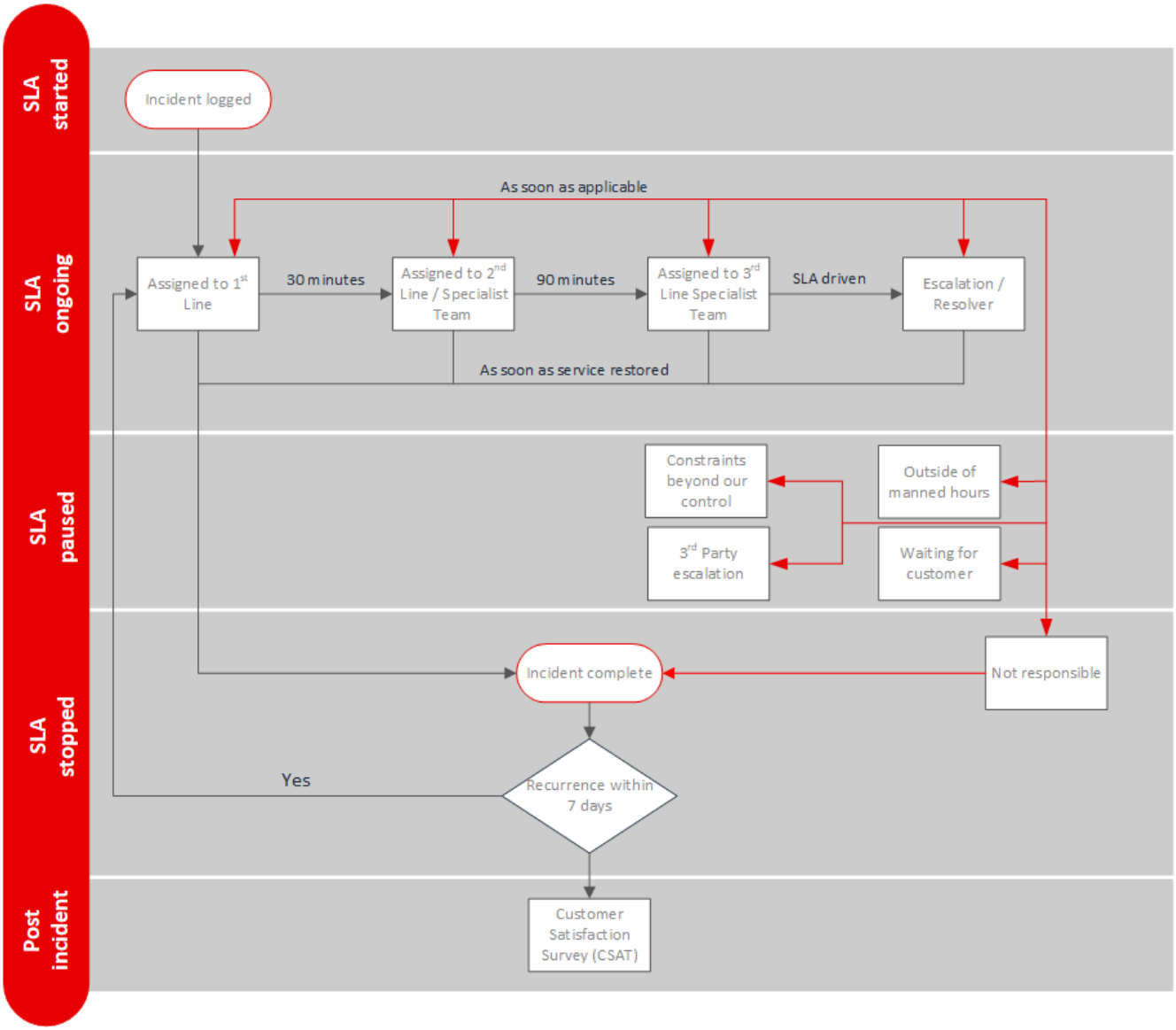
3.7 Ticket Handling & Escalation

3.7.1 P1 and P2 Ticket Flow

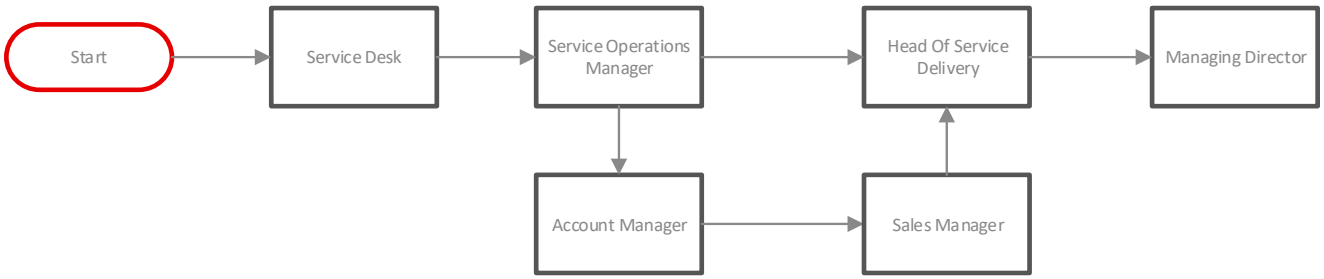


Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

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