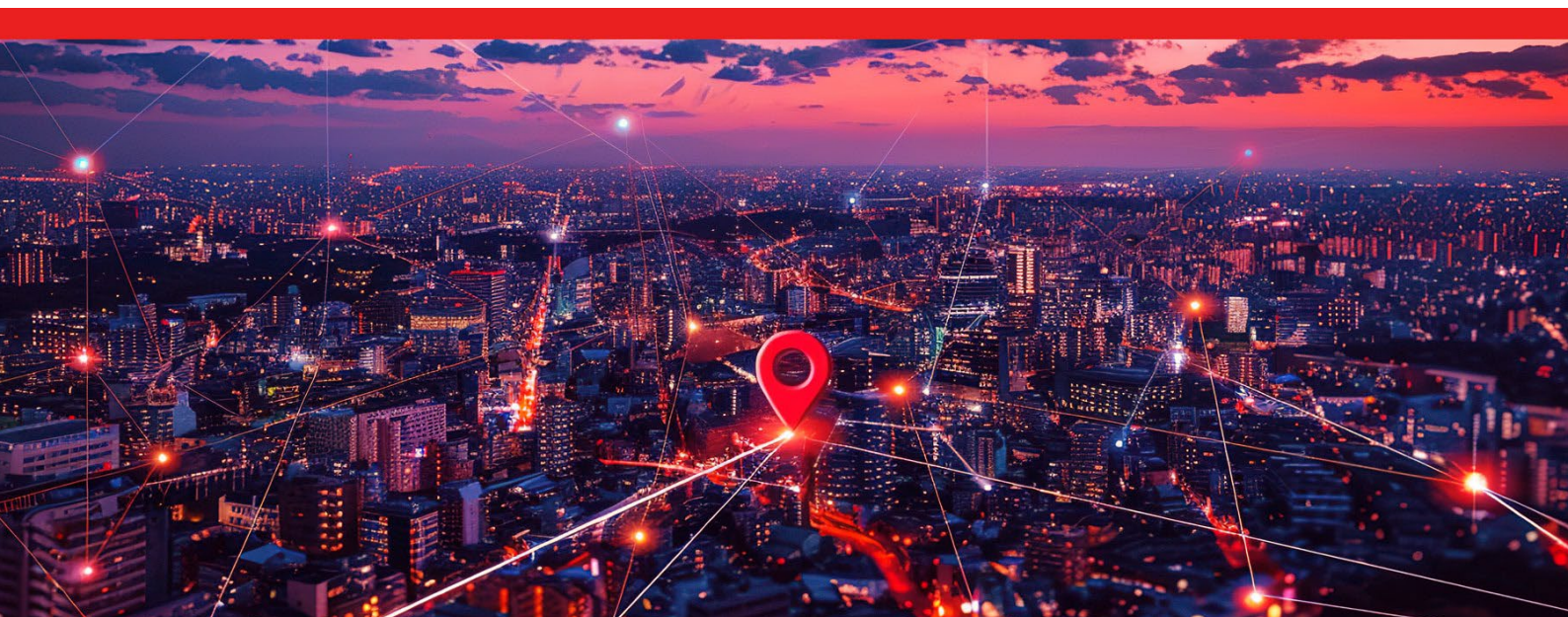


Koris365 Network & Security Resolve

Service Description



Copyright

The information contained in this document is the property of Koris365, a trading name of Koris365 UK Limited. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means; electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Koris365. Legal action will be taken against any infringement.

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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 Executive Summary.....	4
1.1 Service Scope Summary	4
2 Service Onboarding & Mobilisation	5
2.1 Onboarding Requirements & Activities.....	5
2.2 Key Operational & Transition Risks	6
2.3 Onboarding & Mobilisation Success Criteria	6
3 Ticket Types & Priority Classification	7
3.1 Incident Tickets.....	7
3.2 Problem Tickets	7
3.3 Third-Party Ticket Management	7
3.4 Incident Management Process	8
3.5 Major Incidents.....	8
3.6 Priority Classification Matrix	9
4 Service Reporting	10
4.1 Monthly Service Report.....	10
4.2 Major Incident Reporting	10
5 Technical Deliverables.....	11
6 Out of Scope.....	13
7 Service Level Agreement (SLA).....	14
7.1 Hours of Service	14
7.2 Response & Restoration	14
7.3 Service Level Measurement.....	14
8 Offboarding	15
8.1 Offboarding Activities.....	15
8.2 Customer Responsibilities	15
8.3 Data Retention & Deletion	15

1 Executive Summary

Koris365 Network & Security Resolve provides rapid access to specialist engineers to restore critical network and security services, reduce downtime, and minimise business disruption.

Our engineers take ownership of incidents affecting areas such as firewalls, WAN, switching, wireless, routing, and security platforms. Using ITIL-aligned processes, we investigate the issue, coordinate restoration, provide regular updates, and work to restore service as quickly as possible.

Where applicable named third parties agreed during onboarding are involved, Koris365 acts as a Single Point of Contact (SPOC), coordinating vendors and escalations on the customer's behalf.

Resolve provides predictable, SLA-backed support to help keep critical infrastructure available and operational.

1.1 Service Scope Summary

Service Scope	Status	Relevant Service	Relevant Service Purpose
Incident, Major Incident and Problem Management	Included	Resolve	Restoration
Major Incident Reporting	Included	Resolve	Restoration
Third-Party Ticket Management	Included	Resolve	Restoration
Service Requests & Changes	Not included	Operate	Administration
Monitoring & Alerting	Not included	Monitor	Detection
Patching & Software/Firmware Updates	Not included	Patch	Maintenance

2 Service Onboarding & Mobilisation

Onboarding prepares Koris365 to deliver Network & Security Resolve by confirming the supported environment, administrative access, customer contacts, third-party dependencies, support processes, and technical information required to provide effective Incident and Problem Management.

A controlled onboarding process will be completed before the service enters Business-as-Usual operation.

2.1 Onboarding Requirements & Activities

The following requirements must be in place for Koris365 to provide the service:

- The supported system is current, in a good operational state, with best-practice configuration, a good standard of accurate documentation, and is covered by manufacturer support.
- Customer stakeholders and subject matter experts are available throughout onboarding.
- Incumbent suppliers or internal teams will participate in transition activities where required.
- The customer has at least one escalation contact and one contact to raise tickets.
- Remote administrator access to all supported assets will be provided.

Following order acceptance, a Project Manager will coordinate onboarding, confirm service readiness and manage the transition to go-live.

Phase	Key Activities
Initiation & Scope Confirmation	Confirm supported assets and services, customer contacts, third parties, and onboarding requirements.
Discovery & Knowledge Transfer	Review the supported environment, documentation, known issues, dependencies, escalation routes, and relevant recovery/failover procedures.
Service Readiness	Validate administrative access, ticket routing, priority and escalation processes, third-party support routes, and required service documentation.
Operational Handover & Hypercare	Transition into live support, address onboarding issues, review initial service performance and formally move into Business-as-Usual operation.

2.2 Key Operational & Transition Risks

Koris365 uses structured discovery, knowledge transfer, access validation and process testing to reduce operational risk during service onboarding.

Risk	Impact	Mitigation
Incomplete or outdated documentation.	Delayed onboarding, diagnosis and restoration.	Environment discovery and documentation validation.
Limited customer or incumbent SME availability.	Knowledge gaps and delayed mobilisation.	Early stakeholder engagement and structured knowledge transfer.
Delayed or incomplete administrative access.	Delayed onboarding, investigation, and restoration.	Access requirements identified and validated before go-live.
Incomplete third-party support information.	Delays when vendor escalation is required.	Validate named third parties, support routes and escalation contacts during onboarding.
Ticket or escalation process misalignment.	Delayed prioritisation or escalation.	Agree ticket logging, Priority 1 and escalation processes before go-live.

2.3 Onboarding & Mobilisation Success Criteria

Onboarding and mobilisation will be considered successful when:

- The supported environment and service scope have been validated.
- Required administrative access has been provided and tested.
- Customer contacts and escalation routes have been agreed.
- Ticket logging, prioritisation and escalation processes have been confirmed.
- Applicable third-party support and escalation routes have been validated.
- Required technical and operational documentation has been captured.
- Service reporting arrangements have been established.
- The service has been formally handed over into Business-as-Usual operation.

3 Ticket Types & Priority Classification

3.1 Incident Tickets

Incident tickets are used for unplanned disruptions to IT services, such as system failures or service outages.

All incidents are logged in our ticket management system and assigned a priority based on the Priority Classification Matrix. The priority is set when the ticket is logged and may be updated if the incident's impact or urgency changes.

3.2 Problem Tickets

Problem tickets are used to identify and manage the underlying causes of incidents. They focus on root cause analysis to help prevent service disruptions from recurring.

Problem Management includes root-cause investigation and recommended corrective actions, but does not automatically include implementation of configuration changes, software or firmware updates, or project work.

3.3 Third-Party Ticket Management

For ticket types included within Resolve, Koris365 coordinates directly with named third-party providers on the customer's behalf, owning and tracking applicable support tickets through to resolution.

Key responsibilities include:

- Centralised ticket management through the Koris365 Service Desk.
- Initial triage and diagnosis.
- Engagement and coordination with named third-party providers.
- Ticket ownership and escalation through to resolution.
- Customer status updates throughout the ticket lifecycle.
- Validation of service restoration before closure.

3.4 Incident Management Process

Koris365 follows a structured incident management process to restore services quickly, maintain clear communication, and ensure incidents are managed consistently.

- **Identify & Log:** Incidents are reported to Koris365 or, where Network & Security Monitor is also purchased, raised following a monitoring alert. The incident is recorded in the ticketing system and categorised appropriately.
- **Prioritise:** Incidents are prioritised according to impact and urgency.
- **Major incident assessment:** Where an incident has significant business impact, it is assessed for Major Incident classification and, where applicable, managed through the enhanced Major Incident process.
- **Diagnose & Escalate:** The Service Desk performs initial diagnosis and assigns or escalates the incident to the appropriate specialist resources where required.
- **Restore & Communicate:** Koris365 investigates the issue, coordinates recovery activities, and keeps relevant stakeholders updated throughout.
- **Validate & Close:** Service restoration is confirmed, the outcome is documented, and the incident is closed once the service is operating effectively.

3.5 Major Incidents

A Major Incident is an urgent, high-impact issue affecting many users, critical services, or core business operations, with the potential to cause financial loss, reputational harm, or regulatory risk. Major Incidents are treated as Priority 1; however, not all Priority 1 incidents are classified as Major Incidents.

Major Incidents are managed with expedited escalation, enhanced communications, and a coordinated recovery response.

3.6 Priority Classification Matrix

Incident priority is determined by assessing Impact and Urgency using the matrix below. Impact is the measure of the effect of an incident on business processes, users, or the IT infrastructure. Urgency is how quickly the incident must be resolved to prevent further losses.

If the Customer requires an incident to be treated as Priority 1 (Critical), the ticket must be raised or followed up by telephone to activate the applicable response and restoration SLAs. Upon receipt of the request, Koris365 will review the ticket, initiate incident management activities, and, where appropriate, adjust the incident priority.

		Impact		
		High All users of a specific service affected. Critical business processes unavailable. Security or compliance incident affecting a supported service.	Medium Multiple users or a VIP affected. Important, but non-critical business processes are unavailable.	Low One or two users affected. Non-essential business processes are unavailable.
Urgency	High Immediate action required; business operations at risk.	Priority 1 (Critical)	Priority 2 (High)	Priority 3 (Medium)
	Medium Issue should be addressed soon but business can continue.	Priority 2 (High)	Priority 3 (Medium)	Priority 4 (Low)
	Low Minimal business impact; can be scheduled.	Priority 3 (Medium)	Priority 4 (Low)	Priority 4 (Low)

4 Service Reporting

4.1 Monthly Service Report

The monthly service report provides an overview of incident activity, SLA and KPI performance, Major Incidents, Problem Management, recurring issues, service risks, customer satisfaction performance and trends, where sufficient survey responses have been received, and agreed improvement actions.

Reports are delivered electronically no later than five working days after the end of each reporting period.

4.2 Major Incident Reporting

If a Priority 1 incident is classified as a major incident, a service or operation was unavailable for a sustained period, and the root cause was not attributable to the customer or a third party, the customer may request a Major Incident Report (MIR).

A MIR provides a clear, executive-level summary of the incident, including its business impact, the actions taken, and the status of resolution activities. Major Incident Reports will be produced within five working days following ticket resolution unless reliance on a third party extends the timescale.

5 Technical Deliverables

The following tables define the key diagnostic and restoration activities undertaken under Network & Security Resolve:

Switch	Included
Switching performance faults	Diagnosing performance issues including interface drops, errors, throughput, utilisation, CPU and memory.
Access faults	Investigating issues relating to layer 2 switching and services including DHCP, access VLANs, Voice VLANs, and port issues.
Routing services faults	Diagnosing issues relating to routing services including dynamic, static, policy-based routing, and first hop redundancy protocols.
Security issues	Troubleshooting security and associated issues including NAC, policy-based security (ACLs), port security, and 802.1x port-based authentication.
Switch connectivity faults	Investigating faults relating to multiple switch connectivity including virtual switching, stacking, 802.1q trunking, VTP and aggregated channels (LACP, PAgP).
Traffic control faults	Troubleshooting performance and configuration issues including STP, broadcasts, network loops, storm control, QoS classification, markings and policies.
Environmental/Hardware faults	Investigating physical and environmental related faults including faulty PSUs, fans, chassis, cabling, and optics.
OS faults	Investigating and identifying OS-related issues including bugs, field notices, interoperability issues and vulnerabilities contributing to an active incident.

WAN	Included
Routing faults	Investigating connectivity issues relating to static, dynamic and policy-based routing across technologies including IPsec VPNs, SD-WAN, MPLS, VPLS and point-to-point connectivity.
Traffic control faults	Investigating issues relating to network reliability, security, performance, and bandwidth including 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 including cabling, optics, and provider equipment.
Environmental/Hardware	Investigating physical and environmental related faults on supported devices including faulty PSUs, fans, sensors, and chassis.
OS faults	Investigating and identifying OS-related issues including bugs, field notices, interoperability issues and vulnerabilities contributing to an active incident.

Wi-Fi	Included
WLAN faults	Diagnosing WLAN issues including client associations, AP joining, wireless coverage, roaming, interference, and performance.
WLC faults	Investigating faults relating to wireless controllers including access, redundancy, DHCP and mobility issues.
Security faults	Troubleshooting security and authentication related issues including RADIUS, LDAP, TACACS, WebAuth bundle, MAC filtering, and access control lists.
Environmental/Hardware	Investigating physical and environmental related faults including faulty PSUs, fans, sensors, and chassis.
OS faults	Investigating and identifying OS-related issues including bugs, field notices, interoperability issues and vulnerabilities contributing to an active incident.

Firewall	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 VPNs such as: VPN client issues, site-to-site VPNs, transform sets, SSL-VPN Portal access, routing, access, and policies.
Network faults	Troubleshooting issues relating to 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 Anti DDoS Protection.
Firewall Management and Log Applications	Investigating issues relating to firewall management and logging applications such as: FMC, WMS, FortiManager, ASDM, FortiAnalyzer, and Dimensions.
Environmental/Hardware faults	Investigating physical and environmental related faults such as: Faulty PSUs, fans, chassis, cabling, and optics.
OS faults	Investigating and identifying OS-related issues including bugs, field notices, interoperability issues and vulnerabilities contributing to an active incident.
Additional Functions/Modules	Diagnosing issues related to additional inbuilt services such as: Wireless controllers and security fabrics.

Identity Management	Included
Access control faults	Investigating faults relating to network 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, third-party authentication servers and protocols, LDAP, RADIUS, TACACS and MFA.
Environmental/Hardware faults	Investigating physical and environmental related faults such as: Faulty PSUs, fans, chassis, cabling, and optics.
OS faults	Investigating and identifying OS-related issues including bugs, field notices, interoperability issues and vulnerabilities contributing to an active incident.

6 Out of Scope

The following items are considered out of scope. This list is provided for guidance and is not exhaustive.

- Audits, surveys, asset management, site attendance, customer training, and project work are not included but can be purchased separately outside the scope of this service.
- Remediation of known pre-existing issues identified before or during service onboarding, issues caused by customer or third-party changes, issues affecting assets not included in the service, or issues arising from improper management of security certificates.
- Temporary or permanent replacement parts and new hardware.
- Troubleshooting of configurations that are unsupported by the manufacturer or do not follow vendor best practice.
- Ticket management for third parties not included during service onboarding.
- Patching, software/firmware updates, and vulnerability remediation are not included within Network & Security Resolve. Where an incident is attributable to an unpatched device, Koris365 will continue to diagnose the incident and attempt service restoration or a suitable workaround. Where an applicable patch or software/firmware update falls within Network & Security Patch scope, it will be delivered under that service where purchased, completed by the customer, or separately authorised as chargeable professional services.
- Routine administration, Service Requests, standard changes, and planned configuration changes are not included within Network & Security Resolve. Where an incident identifies a requirement for ongoing administration or a permanent configuration change beyond the immediate restoration of service, this will be delivered under Network & Security Operate where purchased, completed by the customer, or separately authorised as chargeable professional services.
- Proactive monitoring, health monitoring, event detection, alerting, and monitoring platform management are not included within Network & Security Resolve. Where Network & Security Monitor is purchased, applicable events may be escalated into Resolve for incident investigation and service restoration. Without Monitor, the customer is responsible for identifying issues and raising incidents with Koris365.

7 Service Level Agreement (SLA)

7.1 Hours of Service

Koris365 offers two service-hour options: Standard Coverage and 24/7 Coverage. The table below outlines the service hours provided under each option.

Service	Monday to Friday 08:00 - 18:00	Monday to Friday 18:00 - 08:00	Weekends	Bank holidays
Standard	P1 – P4 tickets	Excluded	Excluded	Excluded
24/7	P1 – P4 tickets	P1 and P2 tickets only	P1 and P2 tickets only	P1 and P2 tickets only

Working hours are aligned to UK local time, using Greenwich Mean Time (GMT) or British Summer Time (BST), as applicable.

7.2 Response & Restoration

Level	Response Time	Update Time	Target Restoration Time
Priority 1 (Critical)	15 minutes	< 1 hour	4 hours
Priority 2 (High)	1 hour	< 2 hours	One working day
Priority 3 (Medium)	4 hours	NA	Three working days
Priority 4 (Low)	One working day	NA	Seven working days

7.3 Service Level Measurement

Response time is measured from when the ticket is successfully logged to the point where the customer is contacted and investigation begins. Target restoration time is measured from when the ticket is successfully logged to the point when service is restored or a suitable workaround is implemented. This may not be a permanent fix, and additional planned work may be required.

During investigation and troubleshooting of a ticket, the SLA Timer will be paused if:

- Koris365 is awaiting information or action from the customer or a third party.
- Restoration has time constraints outside of our control, for example, non-redundant systems, backup system limitations, third-party SLAs and patching cycles.

Once information has been received, or the requested action has been taken, the SLA Timer will continue.

Response and Restoration SLAs only apply within contracted hours of service.

Target Key Performance Indicator (KPI) for response and restoration SLAs is 95%.

8 Offboarding

Upon termination or expiration of Network & Security Resolve, Koris365 will facilitate an orderly transition of the service. Following completion of offboarding, Koris365 will have no ongoing responsibility for Incident Management, Problem Management or service restoration under Resolve. Any other contracted Koris365 services will remain unaffected.

8.1 Offboarding Activities

The following activities may be performed as part of the offboarding process:

- Provision of current network, infrastructure, and system documentation maintained under the service agreement.
- Transfer of administrative credentials, licences, and service account information owned by the customer.
- Handover of configuration details for supported systems, cloud services, and security platforms.
- Removal of Koris365 administrative access that is no longer required for any remaining contracted services.
- Reasonable transition assistance with the customer's internal IT team or designated replacement provider for a period of up to five working days following service termination.
- Delivery of a final service summary, including open issues, outstanding risks, and unresolved support requests.

Any transition support, project work, documentation updates, data migration assistance, or knowledge transfer activities that Koris365, acting reasonably, determines to be outside the agreed scope, or unreasonable in nature, complexity, or volume, will be provided on a time-and-materials basis and charged at Koris365's prevailing professional services rates.

8.2 Customer Responsibilities

The customer is responsible for:

- Appointing an authorised contact for transition coordination.
- Planning migration of customer data in advance of termination of service.
- Ensuring receipt and secure storage of all transferred credentials and documentation.
- Arranging any required licensing transfers or third-party vendor account ownership changes.
- Confirming completion of the offboarding process within the agreed transition period.
- Changing passwords and disabling accounts as necessary for security purposes.

8.3 Data Retention & Deletion

Customer data will be retained and deleted in accordance with applicable legislation and Koris365 retention policies.

Requests for the latest Customer Data backup must be received within 10 days of service termination or expiry. If no request is received, the data may be deleted.