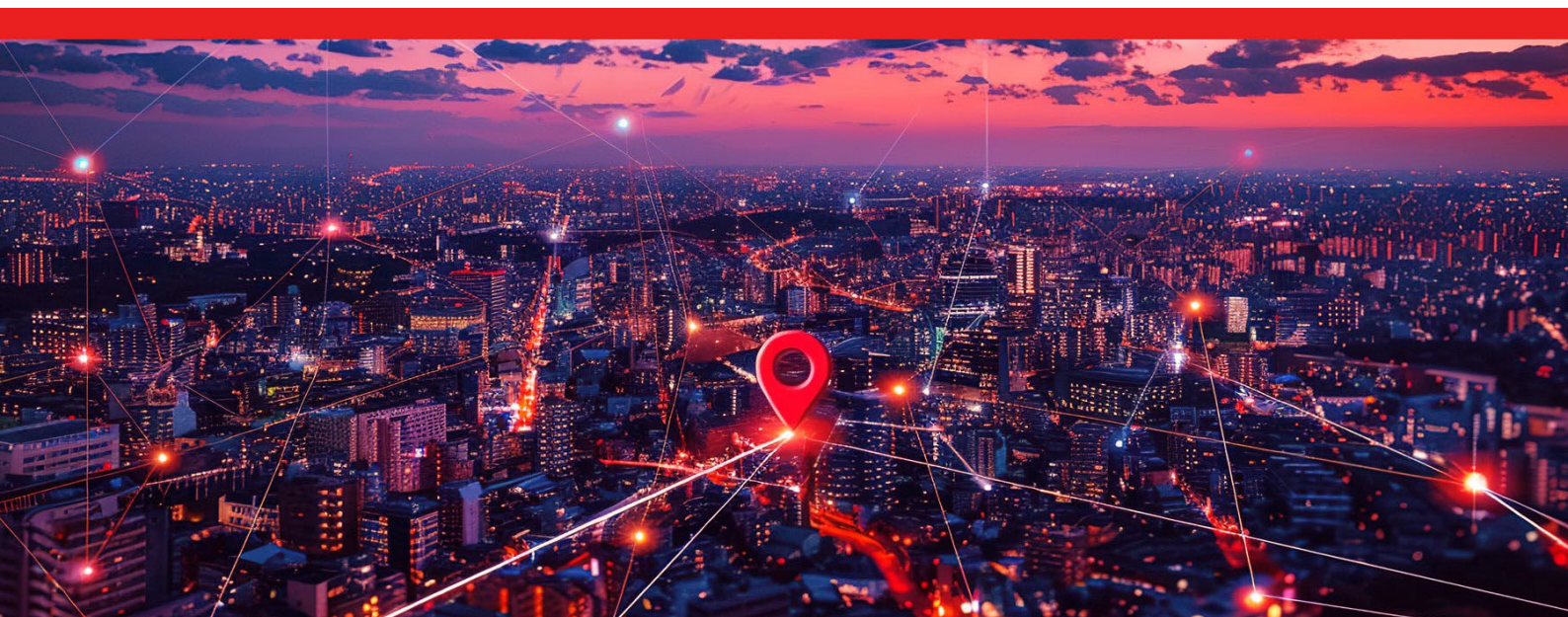


Koris365 Network & Security Operate

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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	Operational Administration.....	7
3.1	Service Requests.....	7
3.2	Standard & Planned Changes	7
3.3	Configuration Management.....	7
3.4	Configuration Backup Management.....	7
4	Service Reporting	8
4.1	Monthly Service Report.....	8
4.2	Quarterly Lifecycle Report	8
5	Technical Deliverables.....	9
6	Out of Scope.....	11
7	Service Level Agreement (SLA).....	12
7.1	Hours of Service	12
7.2	Response & Completion.....	12
7.3	Service Level Measurement.....	12
8	Offboarding	13
8.1	Offboarding Activities.....	13
8.2	Customer Responsibilities	13
8.3	Data Retention & Deletion	13

1 Executive Summary

Koris365 Network & Security Operate provides the day-to-day administration of supported network and security infrastructure, helping customers maintain configuration, fulfil routine Service Requests, and implement controlled changes.

Our engineers administer supported switching, WAN, wireless, firewall, and Identity Management technologies in accordance with agreed operational and change processes.

Operate also provides management of configuration backups for supported devices, helping maintain current configuration data where the technology supports this capability.

1.1 Service Scope Summary

Service Scope	Status	Relevant Service	Relevant Service Purpose
Service Requests & Routine Administration	Included	Operate	Administration
Standard & Planned Configuration Changes	Included	Operate	Administration
Configuration Management	Included	Operate	Administration
Configuration Backup Management	Included	Operate	Administration
Incident Investigation & Service Restoration	Not included	Resolve	Restoration
Monitoring & Alerting	Not included	Monitor	Detection
Patching & Software/Firmware Updates	Not included	Patch	Maintenance

Prerequisite: Network & Security Monitor must be in place for the supported environment.

2 Service Onboarding & Mobilisation

Onboarding prepares Koris365 to deliver Network & Security Operate by confirming the supported environment, administrative access, customer contacts, change and approval processes, configuration information, and operational procedures required to safely administer the service.

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 devices and services have been identified and accurately documented.
- Network & Security Monitor has been implemented for the supported environment.
- The supported environment is in a good operational state, follows vendor best practice, and is covered by appropriate manufacturer support.
- Required administrative accounts, credentials, and remote access are provided.
- Customer contacts authorised to raise Service Requests and approve changes are identified.
- Applicable change approval processes and maintenance requirements are agreed.
- Existing configuration and configuration backup arrangements are available for review.
- An agreed customer-owned configuration backup platform or repository is available and accessible to Koris365.

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, authorised requestors, change approval routes, and onboarding requirements.
Discovery & Knowledge Transfer	Review the supported environment, documentation, configurations, known issues, dependencies, operational procedures, and configuration backup arrangements.
Service Readiness	Validate administrative access, Network & Security Monitor coverage, ticket routing, change processes, configuration information, and required service documentation.
Operational Handover & Hypercare	Transition into live administration, address onboarding issues, review initial service activity, 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 inaccurate documentation	Service Requests or changes may be delayed or carry increased risk.	Validate the supported environment and documentation during onboarding.
Delayed or incomplete administrative access	Koris365 may be unable to administer supported systems.	Identify and validate required access before go-live.
Pre-existing faults or unsupported configurations	Changes may introduce increased operational risk or have unpredictable results.	Identify known issues and configuration concerns during onboarding.
Unclear change authority or approval processes	Changes may be delayed or incorrectly authorised.	Confirm authorised contacts and change approval routes before go-live.
Incomplete configuration backup arrangements	Configuration recovery or rollback may be restricted.	Validate applicable configuration backup capability during onboarding.

2.3 Onboarding & Mobilisation Success Criteria

Onboarding and mobilisation will be considered successful when:

- The supported environment and service scope have been validated.
- Network & Security Monitor is operational for the supported environment.
- Customer-owned configuration backup arrangements have been validated.
- Required administrative access has been provided and tested.
- Authorised customer contacts and change approval routes have been agreed.
- Ticket logging and Service Request processes have been confirmed.
- Required configuration and operational documentation has been captured.
- The service has been formally handed over into Business-as-Usual operation.

3 Operational Administration

Network & Security Operate provides routine administration and controlled configuration changes for supported network and security infrastructure. Activities are initiated through authorised Service Requests and delivered in accordance with agreed customer approval and change processes.

3.1 Service Requests

Service Requests are used for routine administrative activities where no fault or service interruption exists. Requests must be raised by an authorised customer contact and will be reviewed to confirm that they fall within the scope of Network & Security Operate.

Service Requests requiring more than one hour of engineering effort may be assessed as project work and become separately chargeable professional services.

3.2 Standard & Planned Changes

Koris365 will implement routine configuration changes to supported systems where they fall within the defined technical deliverables.

Changes will be:

- Reviewed to confirm scope and technical feasibility.
- Authorised in accordance with the agreed customer approval process.
- Scheduled within the contracted Network & Security Operate service hours, at an agreed time where required to minimise operational impact.
- Implemented using appropriate configuration and rollback procedures.
- Recorded within the relevant ticket and service documentation.

Changes that are complex, high-risk, require significant design work, or fall outside the defined Operate scope may be assessed as project work and separately chargeable professional services.

3.3 Configuration Management

Koris365 will maintain relevant configuration information and service documentation following changes delivered through Network & Security Operate.

Where a change affects the documented supported environment, applicable records will be updated to reflect the implemented configuration.

3.4 Configuration Backup Management

Koris365 will configure and manage backups of supported device configurations to the agreed customer-owned backup platform or repository, where supported by the technology.

The customer is responsible for providing and maintaining the backup platform, including appropriate licensing, capacity, availability, and retention.

4 Service Reporting

Koris365 provides operational reporting to give customers visibility of activity and service performance delivered through Network & Security Operate.

4.1 Monthly Service Report

The monthly service report provides an overview of:

- Service Request activity.
- Standard and planned changes completed during the reporting period.
- Service level performance.
- Configuration backup exceptions, where applicable.
- Outstanding operational risks or actions.
- Agreed service improvement actions.
- Customer satisfaction performance and trends, where sufficient survey responses have been received.

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

4.2 Quarterly Lifecycle Report

The quarterly lifecycle report provides visibility of the lifecycle status of supported network and security assets, including applicable end-of-life or end-of-support information.

Assets will be presented using a Red, Amber, Green status to highlight devices requiring attention or future lifecycle planning.

5 Technical Deliverables

The following tables define the key administration and configuration activities undertaken under Network & Security Operate:

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 VLANs, port security, SD-Access.
Traffic Control Management	Configuration or addition of VLANs, 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.
Licence Management	Smart licensing, applying licences.
Backup Management	Daily configuration backups to the agreed customer-owned backup platform or repository.

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.
Licence Management	Smart licensing, applying licences.
Backup Management	Daily configuration backups to the agreed customer-owned backup platform or repository.

Wi-Fi	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 synchronisation, 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, VLANs, SD-Access.
Licence Management	Smart licensing, applying licences.
Backup Management	Daily configuration backups to the agreed customer-owned backup platform or repository.

Firewall	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, interfaces, VLANs, SD-WAN.
Application Control Management	Configuration of security features including Intrusion Prevention, antivirus, web filtering, advanced malware protection, DNS filtering, Web Application Firewall, endpoint control, and anti-spam.
Licence Management	Smart licensing, applying licences.
Backup Management	Daily configuration backups to the agreed customer-owned backup platform or repository.

Identity 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.
Licence Management	Smart licensing, applying licences.
Backup Management	Daily configuration backups to the agreed customer-owned backup platform or repository.

6 Out of Scope

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

- Incident investigation, Problem Management, Major Incident Management, and service restoration are not included. Where Network & Security Resolve is purchased, applicable incidents will be managed under that service; otherwise, investigation and restoration remain the customer's responsibility.
- Patching, software/firmware updates, and vulnerability remediation are not included. Where Network & Security Patch is purchased, applicable activities will be delivered under that service; otherwise, they remain the customer's responsibility or may be separately authorised as chargeable professional services.
- Deployment of new sites, new infrastructure, major migrations, solution design, or other project activity is not included but can be purchased separately outside the scope of this service.
- Site attendance, audits, surveys, training, disaster recovery planning, and disaster recovery testing are not included but can be purchased separately outside the scope of this service.
- Provision, licensing, capacity, availability, and retention of the customer-owned configuration backup platform are the customer's responsibility. Operate includes management of configuration backups for supported devices only.
- Licence provision and Software Asset Management are not included within Network & Security Operate. Koris365 can supply applicable licences separately where required, but responsibility for licence ownership and compliance remains with the customer.
- Administration of unsupported or end-of-life systems, or configurations that are not supported by the vendor, is not included unless specifically agreed.
- Koris365 will not implement changes considered to present an unacceptable operational risk where suitable contingency or rollback arrangements are not available.

7 Service Level Agreement (SLA)

7.1 Hours of Service

Service	Monday to Friday 08:00 - 18:00	Monday to Friday 18:00 - 08:00	Weekends	Bank holidays
Network & Security Operate	Included	Excluded	Excluded	Excluded

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

Changes required outside standard service hours may be separately scheduled as chargeable professional services.

7.2 Response & Completion

All Network & Security Operate tickets are treated as standard Service Requests. Incident priority classifications do not apply to Operate.

Request Type	Response Time	Target Completion Time
Service Request	One working day	Five working days

Target completion applies to requests within the standard Operate scope. Planned changes requiring an agreed implementation date will be completed at the scheduled time.

7.3 Service Level Measurement

Response time is measured from successful logging of the request to Koris365 contacting the customer or beginning work. Target completion is measured from successful logging to completion of the agreed activity.

The SLA timer will pause while Koris365 is awaiting customer or third-party information, approval or action, an agreed implementation window, or resolution of a dependency outside Koris365's control.

Response and completion SLAs apply only during Network & Security Operate service hours.

Target KPI for response and completion SLAs is 95%.

8 Offboarding

Upon termination or expiration of Network & Security Operate, Koris365 will facilitate an orderly transition of the service. Following completion of offboarding, Koris365 will have no ongoing responsibility for routine administration, Service Requests, configuration changes, or configuration backup management under Operate. 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 configuration and service documentation maintained under the service agreement.
- Transfer of customer-owned credentials or service account information held by Koris365, where applicable.
- Handover of relevant configuration information for supported systems.
- Confirmation of configuration backup arrangements within the customer-owned backup platform.
- 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 summary of open Service Requests, planned changes, outstanding risks, and unresolved actions.

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.
- Ensuring receipt and secure storage of transferred credentials and documentation.
- Maintaining the customer-owned configuration backup platform.
- Arranging any required licence 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.