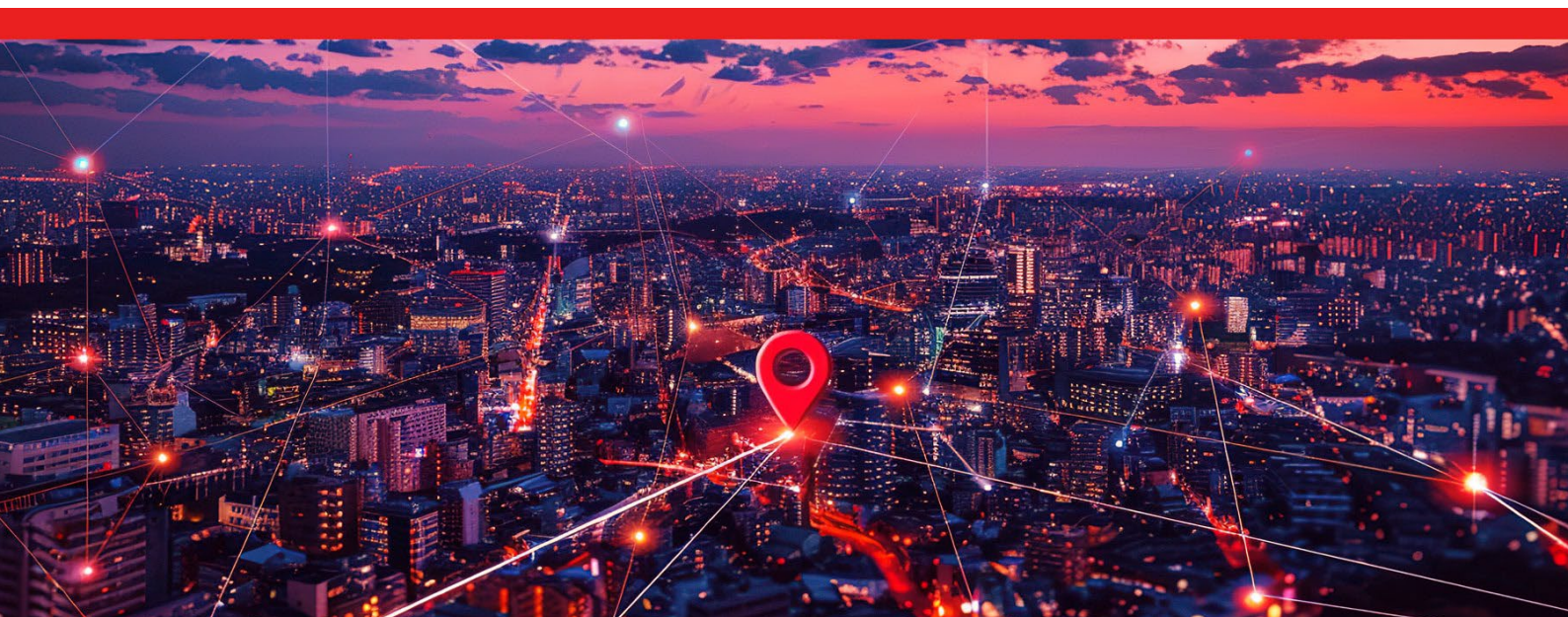


Koris365 Network & Security Patch

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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 Patch Management.....	7
3.1 Vendor Advisory & Vulnerability Review	7
3.2 Routine Patching & Updates.....	7
3.3 High & Critical Vulnerability Remediation.....	7
3.4 Planned Release Activities	7
3.5 Rollback	7
4 Service Reporting	8
4.1 Quarterly Patch & Version Report	8
5 Technical Deliverables.....	9
6 Out of Scope.....	10
7 Service Level Agreement (SLA).....	11
7.1 Hours of Service	11
7.2 Maintenance Scheduling.....	11
7.3 Service Level Measurement.....	11
8 Offboarding	12
8.1 Offboarding Activities.....	12
8.2 Customer Responsibilities	12
8.3 Data Retention & Deletion	12

1 Executive Summary

Koris365 Network & Security Patch provides planned software and firmware maintenance for supported network and security infrastructure, helping customers maintain supported versions, remediate vendor-identified vulnerabilities, and reduce the operational and security risks associated with outdated software.

Koris365 reviews applicable vendor updates and security advisories, identifies relevant remediation for supported devices, and coordinates the deployment of patches, firmware, and software updates through agreed maintenance windows.

The service also provides visibility of software and firmware versions across the supported estate to help customers understand patch status and identify devices requiring maintenance.

1.1 Service Scope Summary

Service Scope	Status	Relevant Service	Relevant Service Purpose
Vendor Advisory & Vulnerability Review	Included	Patch	Maintenance
High & Critical Vulnerability Remediation	Included	Patch	Maintenance
Routine Patching & Software/Firmware Updates	Included	Patch	Maintenance
Planned Release Activities	Included	Patch	Maintenance
Patch & Version Reporting	Included	Patch	Maintenance
Incident Investigation & Service Restoration	Not included	Resolve	Restoration
Monitoring & Alerting	Not included	Monitor	Detection
Service Requests & Configuration Changes	Not included	Operate	Administration

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

2 Service Onboarding & Mobilisation

Onboarding prepares Koris365 to deliver Network & Security Patch by confirming the supported environment, current software and firmware versions, administrative access, maintenance windows, recovery arrangements, and technical information required to safely maintain supported devices.

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 devices and services to be patched have been identified and accurately documented.
- Network & Security Monitor has been implemented for the supported environment.
- Supported devices are covered by appropriate manufacturer support and can receive applicable updates.
- Required administrative accounts, permissions, connectivity, and vendor access are provided.
- Current software and firmware versions are available for review.
- Customer contacts authorised to approve maintenance activity and agree the maintenance schedule and windows are identified.
- Appropriate backup, recovery, or rollback arrangements are available.
- Any significant existing patch backlog or unsupported software identified during onboarding is agreed for remediation before Business-as-Usual patching begins.

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, customer contacts, maintenance requirements, approval routes, and onboarding requirements.
Discovery & Baseline Review	Review current software/firmware versions, vendor support status, known vulnerabilities, dependencies, documentation, and recovery arrangements.
Service Readiness	Validate administrative access, Network & Security Monitor coverage, connectivity, maintenance windows, vendor access, and applicable rollback arrangements.
Operational Handover & Hypercare	Agree the maintenance schedule and initial patching activity, address onboarding issues, 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
Significant patch backlog	Devices may require additional remediation before routine patching can begin.	Review patch levels during onboarding and agree remediation activity before go-live.
Unsupported or end-of-life software	Required patches or vendor support may not be available.	Validate software, firmware, and vendor support status during onboarding.
Delayed or incomplete administrative access	Patching activity may be delayed or unable to proceed.	Identify and validate required access before go-live.
Application or technology dependencies	Updates may affect interoperability or service availability.	Review known dependencies and applicable vendor guidance before deployment.
Insufficient recovery or rollback arrangements	Recovery may be restricted if an update is unsuccessful.	Validate appropriate backup, recovery, or rollback arrangements before patching.
Unavailable maintenance windows or customer validation	Planned patching may be delayed.	Agree maintenance windows, approval routes, and validation responsibilities during onboarding.
Patch-related service impact	A patch or update may cause service degradation, failure, or unexpected behaviour.	Validate rollback arrangements before deployment.

2.3 Onboarding & Mobilisation Success Criteria

Onboarding and mobilisation will be considered successful when:

- The supported environment and patching scope have been validated.
- Network & Security Monitor is operational for the supported environment.
- Current software and firmware versions and vendor support status have been captured.
- Required administrative access and connectivity have been tested.
- Any significant patch backlog or unsupported software has been identified and an agreed remediation approach established.
- The maintenance schedule, maintenance windows, and customer approval routes have been agreed.
- Appropriate rollback arrangements have been validated to return affected systems to their pre-change state if required.
- The service has been formally handed over into Business-as-Usual operation.

3 Patch Management

Patch activity is based on applicable vendor releases, security advisories, the supported environment, and agreed maintenance requirements.

3.1 Vendor Advisory & Vulnerability Review

Koris365 will review relevant vendor security advisories and software releases for supported devices as part of the ongoing service to identify applicable vulnerabilities classified by the vendor as High or Critical and determine any required remediation.

Where an applicable High or Critical vulnerability requires action, Koris365 will notify the customer when identified rather than waiting for the next scheduled report.

3.2 Routine Patching & Updates

Applicable patches and software or firmware updates will be reviewed for applicability and vendor support, implemented using vendor-supported procedures, documented, and validated following deployment using available system and monitoring information.

3.3 High & Critical Vulnerability Remediation

Where an applicable vulnerability is classified by the vendor as High or Critical, Koris365 will assess the required remediation and target deployment within 14 days of the applicable vendor fix or update becoming available, subject to customer approval, vendor availability, and an agreed maintenance window.

Remediation under Network & Security Patch may include applicable software or firmware updates. Where remediation requires a configuration change, this will be delivered under Network & Security Operate where purchased or completed by the customer.

3.4 Planned Release Activities

Koris365 will periodically review the software and firmware versions operating across the supported estate and identify applicable vendor-recommended updates.

Where an update is recommended, Koris365 will agree the implementation approach and maintenance window with the customer before deployment.

3.5 Rollback

Appropriate rollback arrangements will be confirmed before patch deployment.

If patching causes an issue, Koris365 will attempt to return the affected system to its pre-change state.

4 Service Reporting

4.1 Quarterly Patch & Version Report

The Quarterly Patch & Version Report is provided electronically every quarter and provides an overview of:

- Current software and firmware versions.
- Patches and updates completed during the reporting period.
- Vendor-rated High and Critical vulnerabilities and remediation status.
- Outstanding or deferred maintenance activity.
- Risks, exceptions, or dependencies affecting patching.

5 Technical Deliverables

The following activities apply to supported switching, WAN, Wi-Fi, firewall, and other network and security technologies agreed during onboarding:

Activity	Included
Vulnerability Notification	Notification of applicable vendor-rated High and Critical vulnerabilities.
Vulnerability Investigation	Identification and assessment of applicable vendor-rated High and Critical vulnerabilities.
Vulnerability Remediation	Remediation through applicable software or firmware updates.
Software/Firmware Review	Review of current versions and applicable vendor recommendations, including upgrade paths where required.
Planned Software/Firmware Updates	Deployment of agreed vendor-supported updates in accordance with the agreed maintenance schedule.

6 Out of Scope

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

- Incident investigation and service restoration are not included. Further investigation or restoration following patch activity will be delivered under Network & Security Resolve where purchased, completed by the customer, or separately authorised as chargeable professional services.
- Routine administration, Service Requests, and configuration changes are not included. Where Network & Security Operate is purchased, applicable activities will be delivered under that service; otherwise, they remain the customer's responsibility.
- Upgrades requiring significant design, migration, compatibility assessment, or project planning, together with new infrastructure or solution redesign, are not included but can be purchased separately outside the scope of this service.
- Formal patch testing or User Acceptance Testing is not included. Standard post-deployment validation will be performed using available system and monitoring information.
- Unsupported or end-of-life systems, software, or firmware are not included unless specifically agreed.
- Host operating system patching is not included.
- Site attendance, audits, surveys, and training are not included but can be purchased separately outside the scope of this service.
- Issues caused by customer or third-party changes are not included within Patch remediation.

7 Service Level Agreement (SLA)

7.1 Hours of Service

Service	Monday to Friday 06:00 - 23:00	Weekends	Bank holidays
Network & Security Patch	Included	Excluded	Excluded

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

7.2 Maintenance Scheduling

Network & Security Patch is a proactive, scheduled service. Incident priority classifications and restoration SLAs do not apply.

Patching and software or firmware updates will be undertaken in accordance with the agreed maintenance schedule and within an agreed maintenance window.

The customer must respond to proposed maintenance windows within 2 working days to enable patching activity to be scheduled.

Vendor-rated High and Critical vulnerability remediation may be scheduled separately from the routine maintenance schedule.

7.3 Service Level Measurement

Delivery of patching activity is measured against the agreed maintenance schedule and maintenance windows.

Scheduled activity may be delayed or rescheduled where Koris365 is awaiting customer or third-party information, approval or action, vendor software availability, an agreed maintenance window, or resolution of a dependency outside Koris365's control.

8 Offboarding

Upon termination or expiration of Network & Security Patch, Koris365 will facilitate an orderly transition of the service. Following completion of offboarding, Koris365 will have no ongoing responsibility for patching, software or firmware maintenance, or vulnerability remediation under Patch. 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 patching and version information maintained under the service agreement.
- Transfer of customer-owned credentials or service account information held by Koris365, where applicable.
- 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 outstanding or deferred patching activity and known vulnerability remediation requirements.

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 any transferred credentials or documentation.
- Assuming responsibility for ongoing patching and vulnerability remediation following service termination.
- 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.