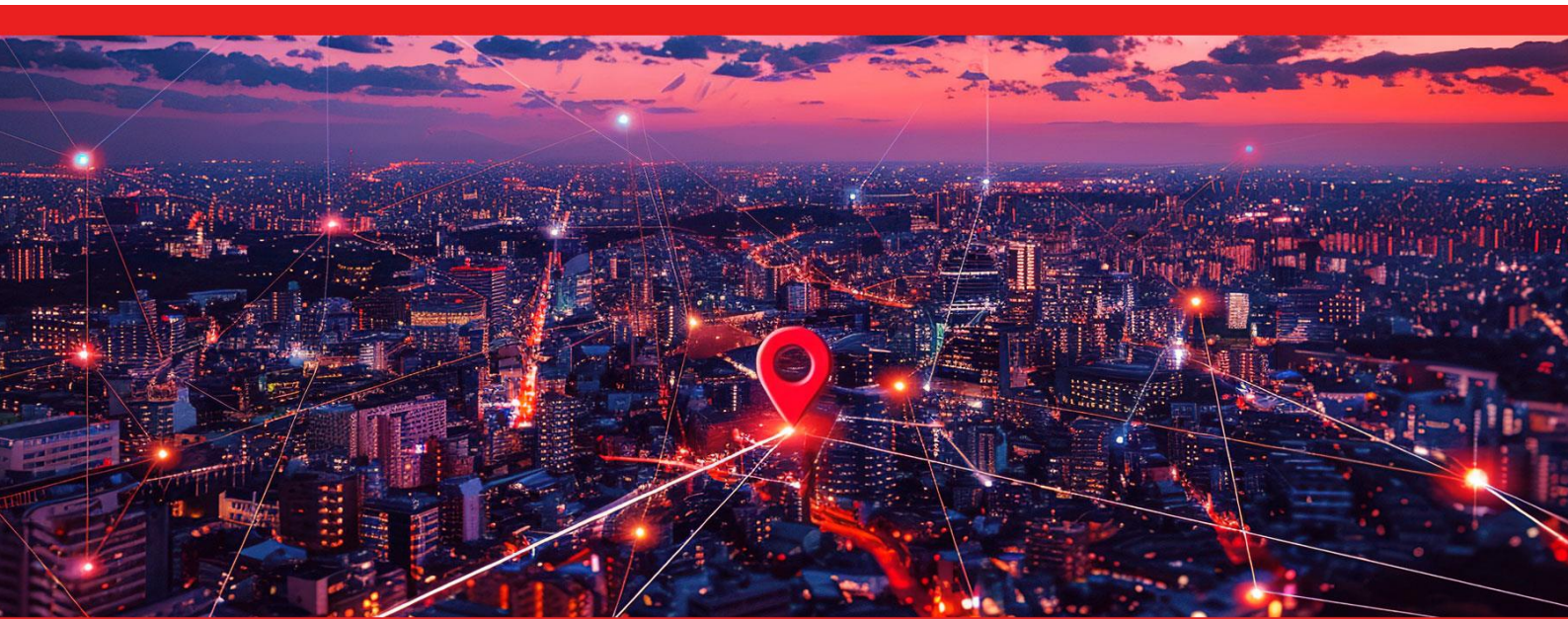# UC Patch

Service Description

Copyright

The information contained in this document is the property of Koris365, a trading name of Koris365 Central Limited, Koris365 South Limited, Koris365 North Limited and Koris365 Ireland 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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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.

Legal Entities

Koris365 is the trading name for the following legal entities:

Koris365 North	Koris365 Central	Koris365 South	Koris365 Ireland
Unit 15 Pavilion Business Park, Royds Hall Lane, Leeds, LS12 6AJ	8 Grovelands, Boundary Way, Hemel Hempstead, HP2 7TE	8 Grovelands, Boundary Way, Hemel Hempstead, HP2 7TE	Trinity House, Charleston Road, Ranelagh, Dublin 6, Ireland, D06 C8X4
Company Reg No: 02276852	Company Reg No: 06215347	Company Reg No: 07709017	Company Reg No: 727514
VAT No: 631921945	VAT No: 912862719	VAT No: 927332425	VAT No: IE04083398OH

IMS101 V1.1

Contents

1   Summary

1.1   Overview

UC Patch is a managed service that can be added to UC Manage to deliver Vendor released security patches, server updates, IOS upgrades, feature enhancements, and fixes.

1.2   Features

UC Patch provides:

- Applicable updates for:
    - Cisco Unified Communication Manager
    - Cisco Unified Presence
    - Cisco Unity Connection
    - Cisco Unified Contact Centre Express
    - Cisco Expressway
    - Cisco Unified Attendant Console
    - Cisco UCS
    - Cisco Cube
    - Mitel MiVoice Business
    - Mitel MiContact Centre Business
    - Mitel Border Gateway
    - Mitel MiCollab
    - Mitel MiVoice Call Recording
    - Mitel Interaction Recording
    - Mitel Open Integration Gateway
    - Ribbon SBC
    - AudioCodes SBC
    - EICC
    - QMS
    - Red Box Recorder
- Quarterly version reporting

1.3   Suitable Customers

Any organisation with a Cisco, Mitel, Microsoft, Enghouse UC solution or Redbox can benefit from UC Patch including:

- Organisations with limited capacity to deliver out of hours maintenance
- Organisations struggling to deploy an effective internal patching solution
- Organisations requiring patching ownership and accountability
- Organisations looking to meet governance requirements by maintaining a security baseline
- Organisations experiencing down-time due to known vulnerabilities of un-patched systems

1.4 Pricing

UC Patch pricing is based on the number and type of devices that require patching.

2 Detailed Service Description

2.1 Pre-requisites

To provide the UC Patch service, Koris365 will require the following:

- UC Manage and UC Resolve
- The customer must provide a comprehensive list of devices to be patched and a good standard of documentation
- Patching must be up to date before take-on or additional costs maybe incurred to bring applications up to required level
- Koris365 must be provided with the necessary service accounts and permissions for the systems that require patching
- Network connectivity will be required
- Firewall modifications may be required
- The customer will need to provide at least one named decision maker
- The customer must provide contact details for at least one technical person who will agree maintenance windows
- The customer may be required to provide a technical person on-site to assist with post-patching testing

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
    d. Application ID's
3. A full audit of the Customer's UC infrastructure may be compulsory depending on the level of information available. The audit is not included in UC Resolve and will be an additional cost to the Customer.
4. Koris365 will work with the customer to complete the Unify 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. Koris365 ensures devices and applications to be patched are at a reasonable patch level
6. If required customer remediates patch level backlog (Koris365 can provide this service at additional cost)
7. Koris365 customer documentation is updated
8. Koris365 agrees service schedule with customer
9. Business as usual patching commences

2.3 Deliverables
2.3.1 Cisco

Cisco Unified Communication Manager	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Device Packs	Biannual installation of vendor released device packs to introduce new devices and existing device firmware updates
DST Updater	Biannual installation of vendor released DST Update COP file to address Daylight Saving Time
Dial Plan Installer	Biannual installation of vendor released dial plans to accommodate new number plans

Cisco Unified Presence	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities

Cisco Unity Connection	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities

Cisco Unified Contact Center Express	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities
DST Updater	Biannual installation of vendor released DST Update COP file to address Daylight Saving Time

Cisco Expressway	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities

Cisco Unified Attendant Console	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities

Cisco Cube	Included
IOS Upgrades	Quarterly upgrade of the vendor recommended IOS to address security vulnerabilities and feature enhancements

2.3.2   Mitel

Mitel MiVoice Business	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Service Packs	Biannual installation of vendor released service packs to introduce bug fixes to core platform and devices. Service Packs to be applied between 06:00 - 23:00 once schedule agreed with customer
Major Releases	Annual upgrade of core platform to include bug fixes and new features. Major Releases to be applied between 06:00 - 23:00 once schedule agreed with customer

Mitel MiContact Centre Business	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Service Packs	Biannual installation of vendor released service packs to introduce bug fixes to core MiCC software and IVR. Service Packs to be applied between 06:00 - 23:00 once schedule agreed with customer
Major Releases	Annual upgrade of core MiCC and IVR software to include bug fixes and new features. Major Releases to be applied between 06:00 - 23:00 once schedule agreed with customer

Mitel MiVoice Border Gateway	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Service Packs	Biannual installation of vendor released service packs to introduce bug fixes to core MBG/MSL software. Service Packs to be applied between 06:00 - 23:00 once schedule agreed with customer
Major Releases	Annual upgrade of core MBG/MSL software to include bug fixes and new features. Major Releases to be applied between 06:00 - 23:00 once schedule agreed with customer

Mitel MiCollab	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Service Packs	Biannual installation of vendor released service packs to introduce bug fixes to core MiCollab/MSL software. Service Packs to be applied between 06:00 - 23:00 once schedule agreed with customer
Major Releases	Annual upgrade of core MiCollab/MSL software to include bug fixes and new features. Major Releases to be applied between 06:00 - 23:00 once schedule agreed with customer

Mitel MiVoice Call Recording and Interaction Recording	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Service Packs	Biannual installation of vendor released service packs to introduce bug fixes to core Call recording software. Service Packs to be applied between 06:00 - 23:00 once schedule agreed with customer
Major Releases	Annual upgrade of core Call recording software to include bug fixes and new features. Major Releases to be applied between 06:00 - 23:00 once schedule agreed with customer

Mitel Open Integration Gateway	Included
Vulnerabilities Patch	Installation of patches released by vendor to address critical security vulnerabilities. Patches to be applied between 06:00 - 23:00 once schedule agreed with customer
Service Packs	Biannual installation of vendor released service packs to introduce bug fixes to core OIG/MSL software. Service Packs to be applied between 06:00 - 23:00 once schedule agreed with customer
Major Releases	Annual upgrade of core OIG/MSL software to include bug fixes and new features. Major Releases to be applied between 06:00 - 23:00 once schedule agreed with customer

2.3.3   Skype for Business

Skype for Business	Included
Server Updates	Quarterly installation of patches released by vendor to address security vulnerabilities and feature enhancements

2.3.4 Ribbon SBC

Ribbon SBC	Included
Firmware Upgrades	Quarterly upgrade of the vendor recommended software to address security vulnerabilities and feature enhancements

2.3.5 AudioCodes SBC

Audiocodes SBC	Included
Firmware Upgrades	Quarterly upgrade of the vendor recommended software to address security vulnerabilities and feature enhancements

2.3.6 Enghouse

EICC	Included
Hotfixes	Quarterly installation of Maintenance Service Pack released by vendor to address bugs, security vulnerabilities, and feature enhancements

QMS	Included
Hotfixes	Biannual installation of Maintenance Service Pack released by vendor to address bugs, security vulnerabilities, and feature enhancements

2.4 Exclusions

- Fault resolutions without exception
- Major release upgrades requiring multi stage upgrades – Koris365 would need to treat as a project and sit out of scope for this service.
- Customer site visits
- Remediation of issues caused by customer or third-party changes
- Testing of patches
- End of Support and End of Software Maintenance applications and system versions
- System builds outside vendor defined standards and not pre-approved by Koris365
- Windows Operating System updates
- Koris365 take no responsibility for the introduction of bugs, loss of service, or the loss of data stored caused by the installation of vendor updates
- Unused maintenance windows will not be rolled over

3 Service Level Agreement (SLA)
3.1 Hours of Service

Service	Mon - Fri	Weekends	Bank holidays
Extended	06:00 - 23:00	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	NA	NA
Priority 2	NA	NA
Priority 3	NA	NA
Priority 4 / Service Requests	Next Business Day	NA

UC Patch is a pro-active service. Tickets are raised as service requests but are instigated by Koris365 rather than the customer. Koris365 will contact the customer in accordance with the agreed schedule to arrange a maintenance window. The customer must respond within a reasonable time frame (48 hours) and permit the maintenance window to occur within the extended hours detailed in section 3.1.

- Koris365 take no responsibility for failure to patch systems where the customer has been unable to agree a maintenance window
- 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
- One service request ticket will be raised per device or application and will remain on hold for the duration
- Koris365 take no responsibility where events outside of our control prevent or interrupt a maintenance window

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 outside of contracted manned hours

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

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 Definitions

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
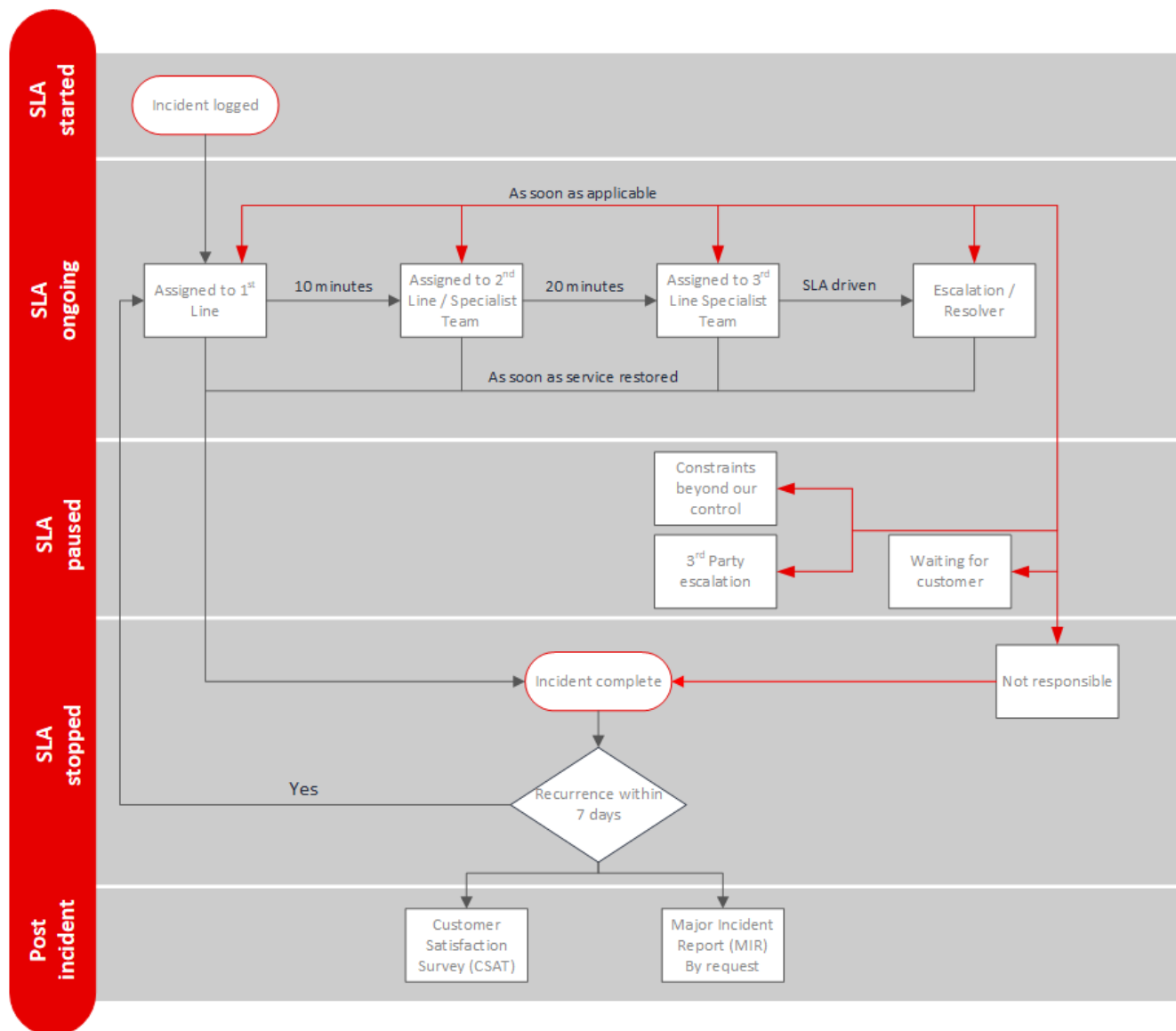
3.7.2 P3 and P4 Ticket Flow
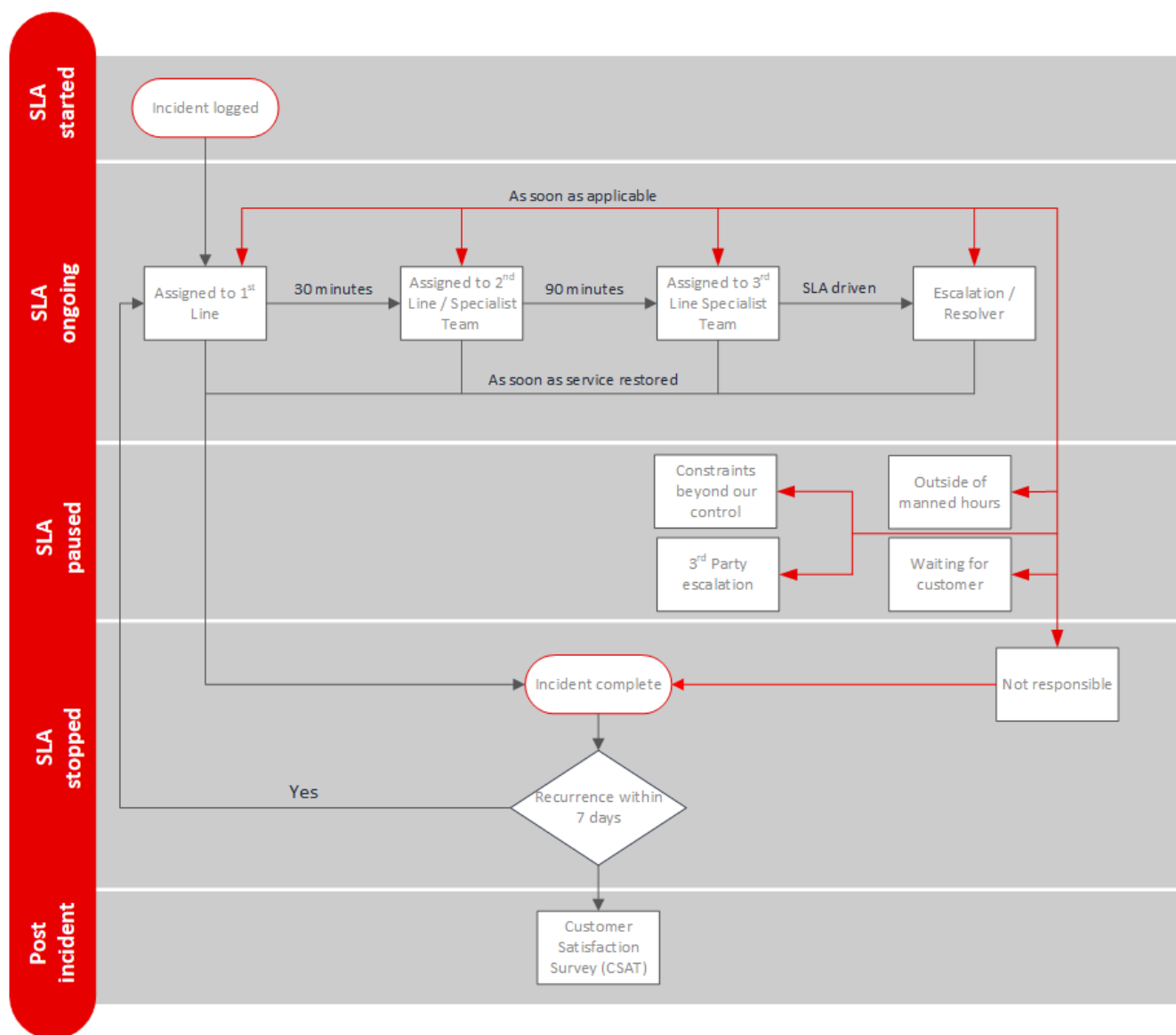
3.7.3 Customer Escalation

IMS101 V1.1
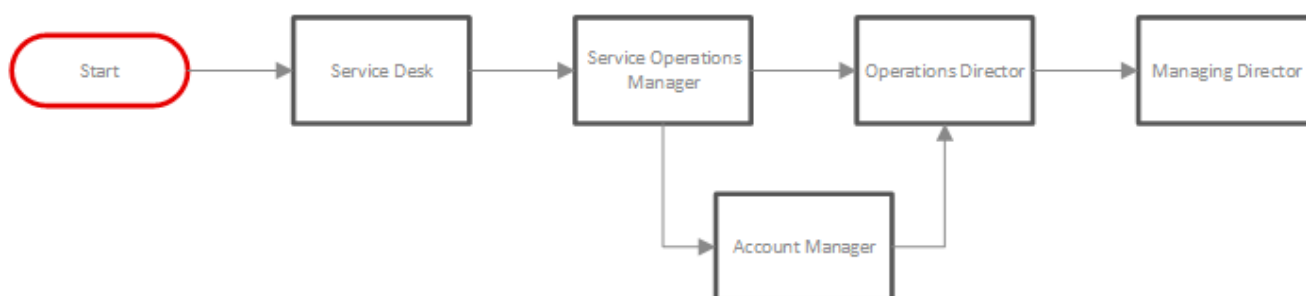
4 Offboarding Procedure

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

IMS101 V1.1