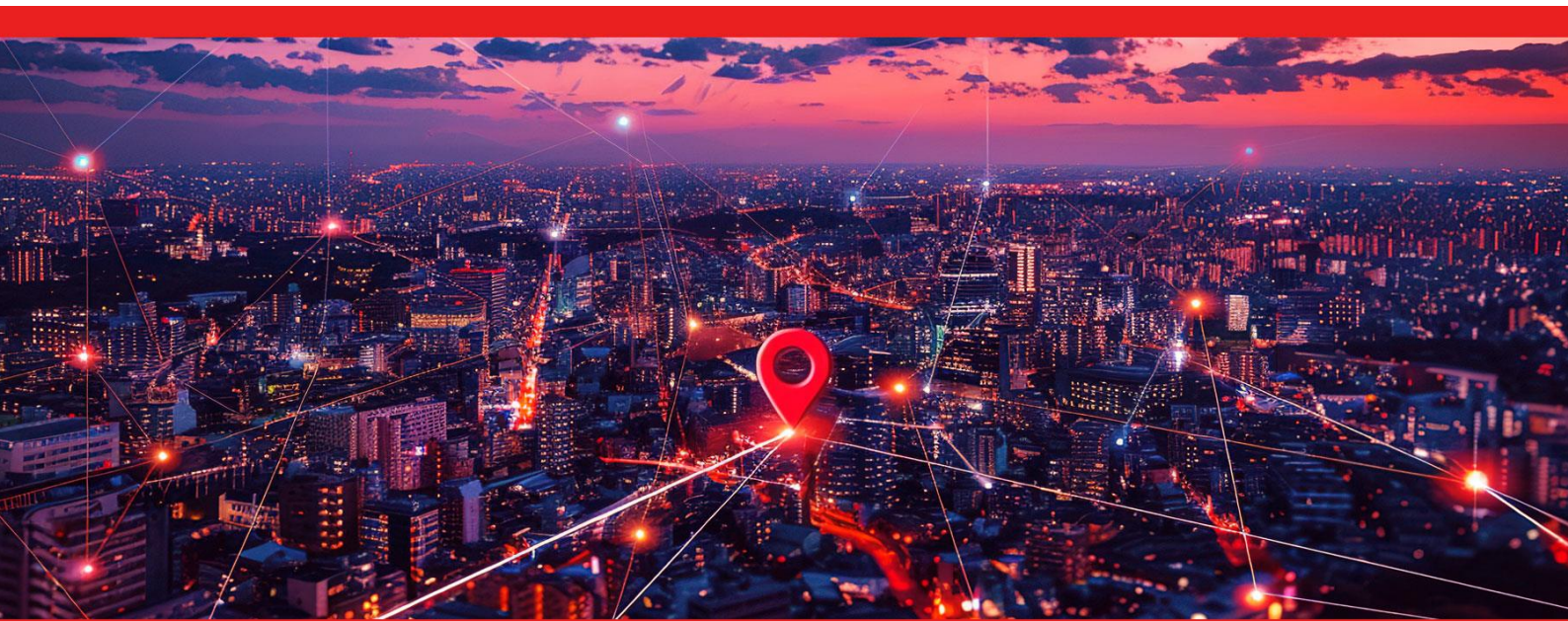# Microsoft 365 Manage & Resolve

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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 VAT No: 631921945	Company Reg No: 06215347 VAT No: 912862719	Company Reg No: 07709017 VAT No: 927332425	Company Reg No: 727514 VAT No: IE04083398OH

Contents

1 Summary

1.1 Overview

Microsoft 365 Manage & Resolve provides management and support of a customer's Microsoft 365 platform. Our dedicated team of IT professionals will assist a customer's IT department, or representative, in resolving issues, managing the platform, as well as providing advice and guidance for Microsoft 365.

1.2 Features

Features available in the Microsoft 365 Manage & Resolve service include:

- Remote support available via telephone, email and customer portal interface
- License procurement and allocation
- Portal and service administration
- Troubleshooting and resolution

1.3 Suitable Customers

Any organisation consuming, or planning a move to, Microsoft 365 can benefit from Microsoft 365 Manage & Resolve including:

- Organisations with limited, or no, IT support resource
- Organisations not skilled in Microsoft 365
- Organisations looking to remove the burden of Microsoft 365 support allowing IT resource to be allocated elsewhere
- Organisations requiring Microsoft 365 ownership and accountability
- Organisations requiring Microsoft 365 support outside of existing IT support resource hours

1.4 Pricing

Microsoft 365 Manage & Resolve pricing consists of a core per company service cost with an additional cost per user.

IMS 102 v1.2

2 Detailed Service Description

2.1 Pre-requisites

To provide the Microsoft 365 Manage & Resolve service, Koris365 will require the following:

- The customer must have an active Microsoft 365 subscription
- Microsoft 365 services must have been deployed and configured correctly
- The customer must provide a good standard of documentation for the current Microsoft 365 deployment
- The customer must provide relevant company detail such as quantity of users, locations, and working hours
- Koris365 must be provided with admin access
- To support hybrid deployments Koris365 may need suitable administrative access to on-premises systems
- Koris365 will need to consume one user license to provide effective troubleshooting
- 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)
- The customer must provide a list of at least one technical person who can assist or take ownership when an issue, or part of, is out of scope

2.2 Onboarding

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) Configurations
3. 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
4. If required, Koris365 make recommendations to remedy any pre-existing faults or misconfigurations
5. If applicable, customer remediates any pre-existing faults or misconfigurations (Koris365 can provide professional services resource at additional cost if required)
6. Koris365 and customer agree on IT procedures e.g. new starters, leavers, permission changes
7. Koris365 customer documentation is updated
8. Customer receives welcome pack including ticket logging instructions
9. Business as usual service commences

2.3 Deliverables

Exchange Online	Included
Hybrid Exchange Server administration and troubleshooting	Troubleshooting, implementing fixes and workarounds, and administering migration endpoints, hybrid configuration, certificate renewals (see exclusions), hybrid mail-flow, and mailbox migrations
Microsoft 365 Mailbox, group, and contact administration	Administration of mailboxes, Microsoft 365 groups, contacts, public folders, and calendars
Mail flow configuration	Administration of Exchange Online connectors, accepted domains, and transport rules
Mail flow troubleshooting	Troubleshooting, implementing fixes and workarounds for mail flow failure
Exchange Online spam and malware filtering	Exchange Online Protection administration, including malware, connection and spam filters, and releasing items from quarantine
Exchange Online compliance management	Administration tasks including discovery searches, litigation hold, management of existing Data Loss Prevention (DLP) policies, administration of retention policies and tags, and journal rules

Azure AD	Included
Azure Active Directory Connect (AADC) troubleshooting and administration	Administering AADC, diagnosing and resolving synchronisation issues
Active Directory Federation Services (ADFS) troubleshooting and administration	Troubleshooting, implementing fixes and workarounds for ADFS and web application proxy roles. Certificate renewals (see exclusions)
Multi-Factor Authentication (MFA) administration	Enabling and disabling of Microsoft 365 MFA against user accounts

Portal Administration	Included
License allocation and management	Allocating and removing user licences
User and group administration	Creation and management of cloud users and groups
Tenancy settings	Managing tenancy security and privacy settings and the organisational profile

MS Teams	Included
Troubleshooting and administration	Administration of Teams, organisation wide settings, user settings, meeting policies, and messaging policies.

SharePoint	Included
Permission administration	Adding and removing user/group permissions from SharePoint libraries, folders, and files
Versioning	Restoring previous versions

OneDrive	Included
Storage quota and access	Administering user settings, storage quotas, data retention, and sync settings

2.4 Exclusions

- Cost of Microsoft 365 Licenses
- Remediating issues caused by customer or third-party changes (this will be considered chargeable)
- Configuration or addition of any backup services (additional professional services and products available)
- Data recovery outside of Microsoft 365's default mechanisms and retention
- Koris365 take no responsibility for the loss of data caused by failures of Microsoft's platform
- Deployment of any previously unconfigured features or services
- Deployment or upgrade of Microsoft 365 ProPlus applications
- Training
- Issues caused by underlying operating systems, hardware, conflicting applications, plugins, malware, performance issues
- On-premises Exchange servers outside of the hybrid configuration
- On-premises Active Directory faults, misconfigurations and administration
- Development
- Certificate management and installation (if not procured through Koris365)
- Issues caused by the improper management of SSL certificates
- Direct end user support (tickets must be raised by named representative who has qualified the issue as Microsoft 365 related)
- This is not a security service. Any ability to provide protection or forensic investigation will be limited by the customers O365 licensing and not guaranteed by Koris365
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Creation of new starters (Koris365 will manage only the Microsoft 365 elements of the process)
- Koris365 take no responsibility for false positives, malware, spam, or users disclosing their passwords
- 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 don't follow vendor best practice

IMS 102 v1.2

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
24/7 (Out of standard hours)	P1 and P2 incidents only	P1 and P2 incidents only	P1 and P2 incidents only

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

- Priority 1 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

IMS 102 v1.2

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 2, 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 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 and an abandoned call rate of less than 8%. An abandoned call is a call where the caller has remained in a queue for at least 15 seconds but has subsequently hung up before speaking to an agent. Abandoned calls are measured between 07:00 – 22:00 Mon - Fri and 08:00 – 17:00 Weekends.

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

IMS 102 v1.2

|	
	• 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)	Servicedesk 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 Process

IMS 102 v1.2
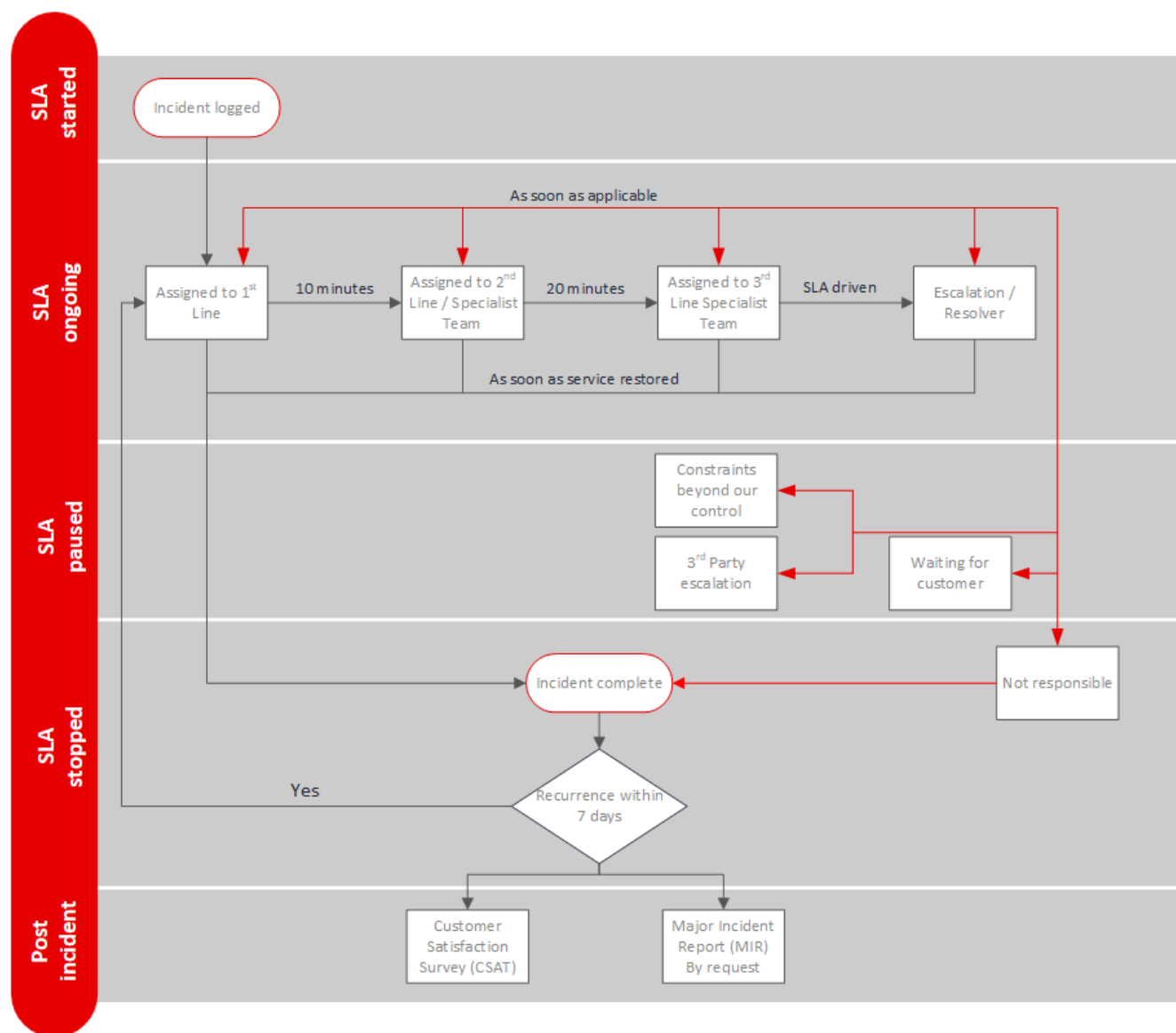
3.7.1 Customer Escalation
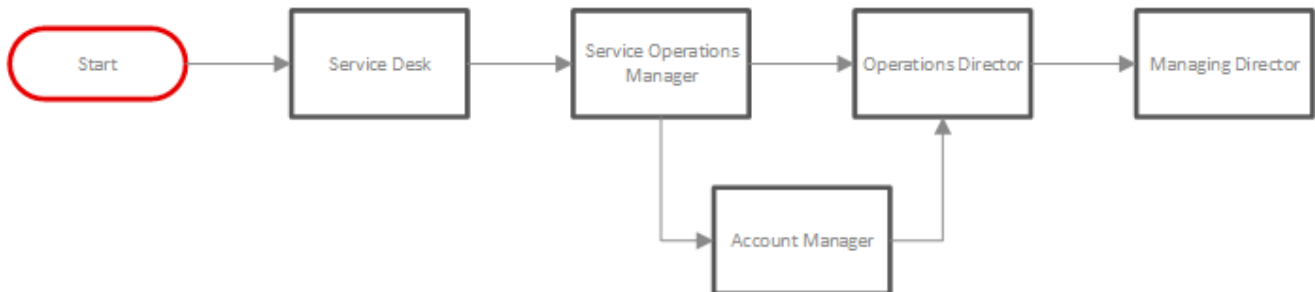
4 Offboarding Procedure

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

IMS 102 v1.2