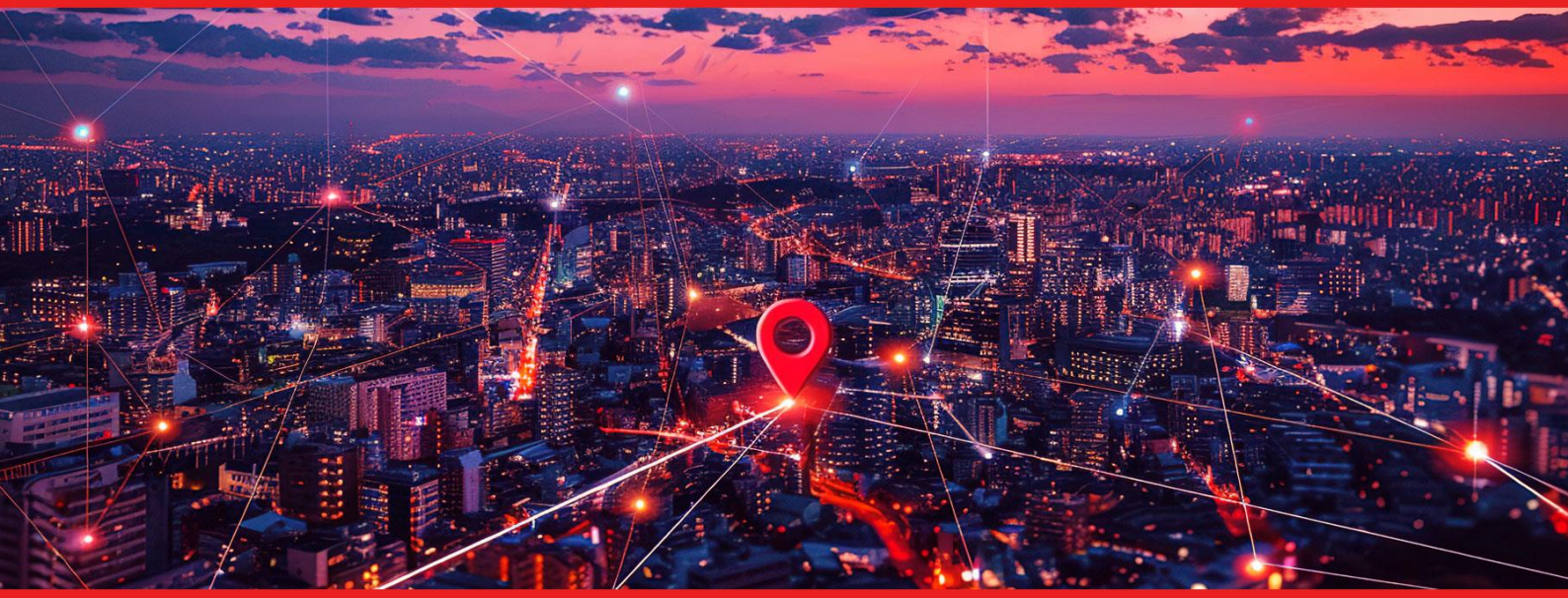
Device Management & Compliance

Service Description



Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

Copyright

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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 Summary

1.1 Overview

Device Management & Compliance provides monitoring and management of a customer's Microsoft Windows device estate. Our dedicated team of IT professionals will administer Microsoft Intune and enrich its capabilities by integrating our remote monitoring and management solution. Koris365 will monitor and remediate device compliance, provide patch management, and provide advice and configuration assistance on securing Microsoft Windows endpoints.

1.2 Features

Features available in the Device Management & Compliance service include:

- Monitoring clients for vulnerabilities and compliance issues.
- Compliance and configuration vulnerability remediation.
- Administering device policies and application deployment.
- Patch Management including common 3rd party applications. See supported 3rd party software patch list here

1.3 Suitable Customers

Any organisation utilising Microsoft Intune and requiring assistance managing their device estate, especially those looking to proactively manage Microsoft Windows secure configuration or maintain security certifications such as Cyber Essentials, can benefit from Device Management & Compliance including:

- Organisations with limited, or no, IT resource
- Organisations who don't have the resources, skills, or tools to be able to manage their devices.
- Organisations looking to remove the burden of device management allowing IT resource to be allocated elsewhere.

1.4 Pricing

Device Management & Compliance pricing consists of a core per company service cost with an additional cost per device.

2 Detailed Service Description

2.1 Pre-requisites

To provide the Device Management & Compliance service, Koris365 will require the following:

- The customer must have an active Microsoft 365 subscription including Intune and Defender for Endpoint (or Defender for Business)
- Microsoft 365 services must have been deployed and configured correctly prior to contract start
- The customer must provide a good standard of documentation for the current Microsoft 365 deployment
- The customer must provide relevant company details 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 or implement some configurations.
- 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 unless combined with "Unify Core End User" service)
- The customer must provide details 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 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

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

3 Deliverables

Intune	Included
Device Administration	Removing retired devices, wiping devices, changing user associations,
Autopilot and Enrolment Configuration	Configuring deployment profiles, automatic enrolment configuration, Enrolment Status Page configuration, enrolment restriction configuration
Management of Configuration Policies	Configuring configuration profiles
Management of Compliance Policies	Configuring compliance policies
Management of endpoint security policy	Configuring Intune endpoint security policies
Application Deployment	Creating/modifying Intune Windows applications
BitLocker Administration	Retrieving BitLocker keys (when stored in Entra ID)
Patch Management	Configuring Windows update rings and Windows Autopatch (subject to licensing)

N-Central	Included
Intune Integration	Integration with Intune to deploy agent to endpoints and monitor metrics such as compliance
Patch Management	Automated patching of supported 3rd party applications
Reporting	Integration with our Brightguage reporting tools
Remote Remediation	Using remote assistance and management tools to remediate compliance issues

Defender	Included
Integration with Intune	Configure integrations with Intune such as device onboarding
Monitor Windows vulnerabilities	Use Defender vulnerability information and device secure score to identify improvements to Intune Endpoint Security policy and out of date software

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)
- Backup or Data recovery
- Koris365 take no responsibility for the loss of data caused by failures of Microsoft's platform.
- Deployment of any previously unconfigured features or services
- Training
- Issues caused by underlying operating systems, hardware, conflicting applications, plugins, malware, performance issues
- 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 Device Management & Compliance related)
- This is not a SOC and/or SIEM service. Any ability to provide protection or forensic investigation will be limited by the customers Microsoft 365 licensing and not guaranteed by Koris365.
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Device lifecycle management, procurement, deployment, etc. Is not a part of this service, those services are offered separately.
- 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.
- Any usage or administration of features not included in the customers Microsoft 365 license.
- Remediating hardware issues with devices.

5 Service Level Agreement (SLA)

5.1 Hours of Service

Service	Mon - Fri	Weekends	Bank holidays
Standard	08:00 – 18:00 manned hours	Excluded	Excluded
Extended	07:00 – 22:00 manned hours	08:00 – 17:00 manned hours	Excluded
24/7	07:00 – 22:00 manned hours On call service outside of manned hours	08:00 – 17:00 manned hours On call service outside of manned hours	On call service

Service hours are based upon GMT/BST time zone

5.2 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

5.3 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.

5.4 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.

5.5 Ticket Types

5.5.1 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 one time, i.e. bulk service requests, will require scheduling.

Where a service request is expected to take more than 1 hour to complete the request will be reviewed and possibly assigned as a separate project.

5.5.2 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.

5.6 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

5.6.1 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

5.6.2 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

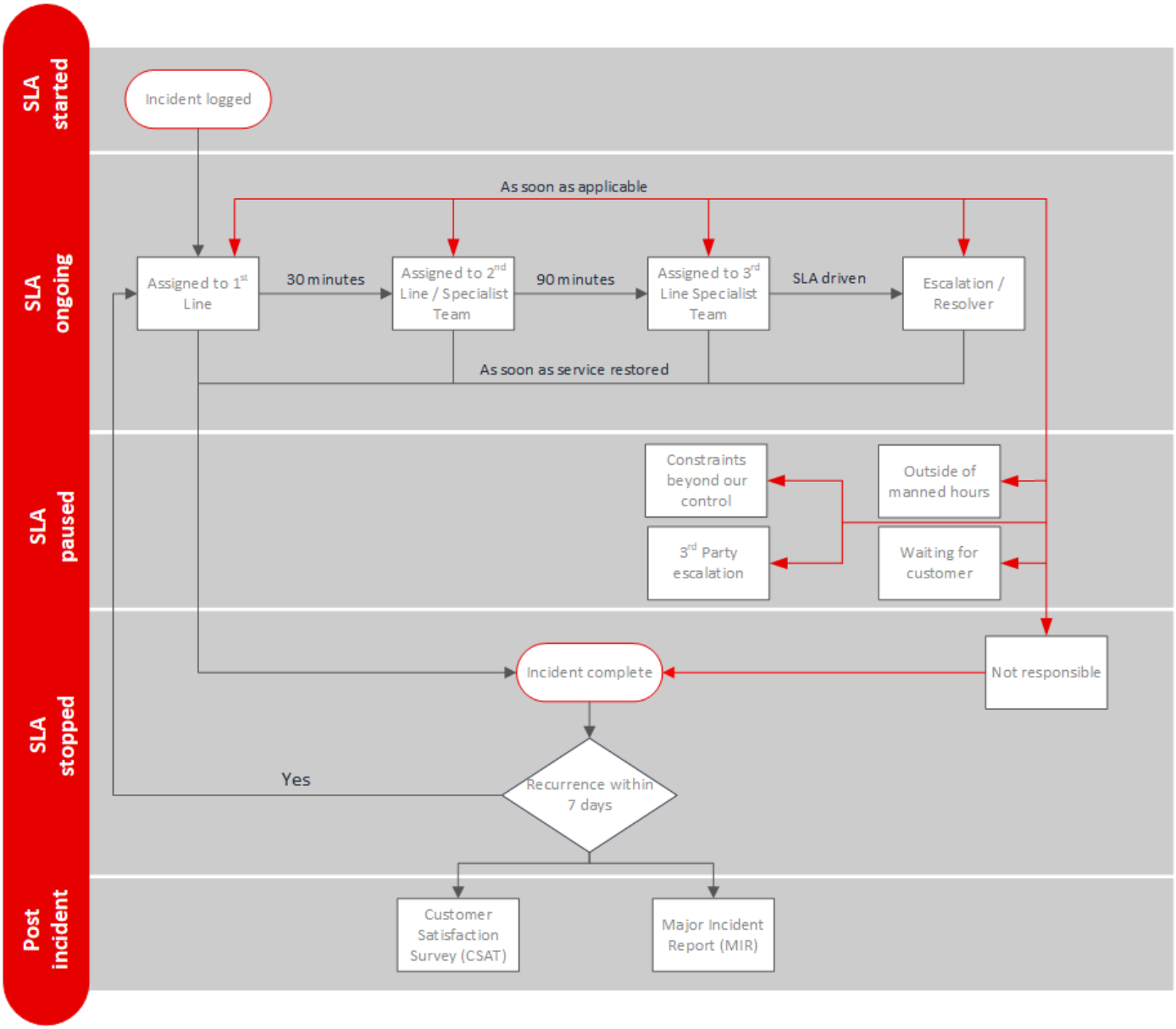
	• Damage to reputation of business is likely to be moderate • A moderate number of customers are affected
Low	• A minimal number of employees are affected • Negligible financial impact • Damage to reputation of business is likely to be minimal • A minimal number of customers are affected

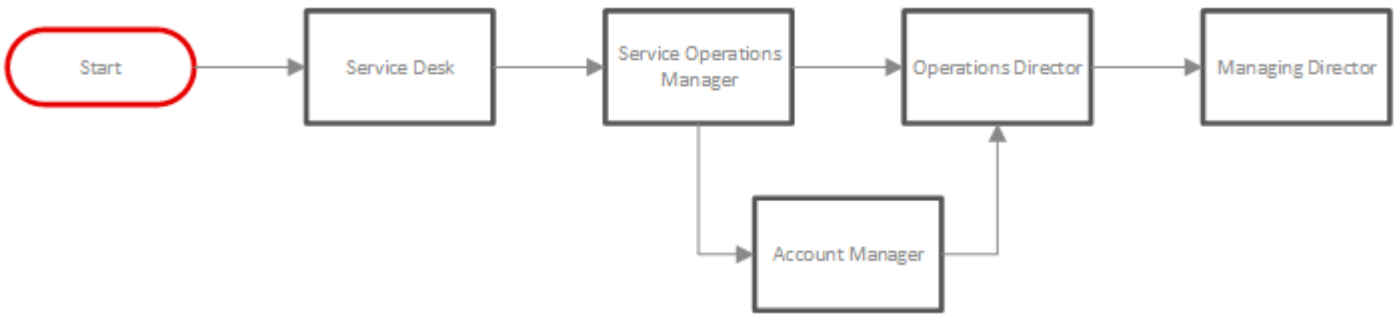
5.6.3 Incident Priority Matrix

		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 immediate, 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

5.7 Ticket Handling & Escalation Process





6 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