GPK Managed Services Agreement (MSA) Coverage Matrix

SCOPE OF WORKS

VERSION |

Table of Contents

GPK Managed Services Agreement (MSA) Coverage Matrix

This matrix outlines the services covered under the GPK Managed Services Agreement (MSA), specifies what is not covered, and indicates when additional fees will apply. It is a comprehensive guide for GPK staff and customers to understand service expectations and billing practices. We aim to ensure transparency, fairness, and alignment between GPK and its customers.

Important Note on Technology Stack Compatibility

GPK's ability to provide full coverage under this MSA is contingent upon the customer's adoption of GPK's recommended technology stack. However, new customers may not initially utilise the full GPK technology stack. During the transition period, GPK agrees to support agreed-upon existing firewalls, switches, wireless access points, backup and archiving solutions, and EDR/XDR solutions that are not part of our standard technology stack. This support will continue until these systems can be replaced with solutions within the GPK technology stack.

End Point Devices

Service/Feature	**Included in GPK's MSA**	**Not Included in GPK's MSA**
Proactive Monitoring & Alerting	Yes, for Windows operating systems still supported by Microsoft and devices monitored via GPK's RMM tool (Automate)	EOL Windows versions, unsupported OS, or devices not monitored by GPK's RMM tool
Operating System Patch Management	Yes, using GPK's deployment tools (ImmyBot, Automate, Intune) for supported Windows OS	Systems not using GPK's deployment tools or unsupported OS versions.
Software Patch Management	Yes, for supported third-party software managed via GPK's deployment tools	Unsupported or custom software not managed by GPK's tools.
Remote Support	Yes, unlimited remote support during business hours	All after-hours support is billable (unless GPK deems otherwise)
Endpoint Management	Yes, for supported Windows endpoints managed through GPK's tools. MacOS if agreed between GPK and customer.	Devices not managed by GPK and devices running Linux, or other unsupported OS
Antivirus/Antimalware Management (SentinelOne)	Yes, SentinelOne managed for supported Windows endpoints	Endpoints without SentinelOne or non-supported antivirus solutions
Cybersecurity Incident Response	GPK's standard Cybersecurity Incident Response requires SentinelOne EDR and Vigilance Response subscriptions to manage and contain security incidents on endpoints and servers.	Advanced Incident Response is a premium, chargeable service not included in GPK's standard Cybersecurity Incident Response offering.
Email Security	Yes, it requires Barracuda Email Protection solutions	Unsupported or third-party email security solutions

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Web Application Firewalls (WAFs)	Yes, it requires Barracuda WAF or agreed-upon WAF devices.	Unsupported WAF solutions
On-premises Hardware Support (End Point Devices)	Yes, for listed MSA devices in head and branch offices using GPK's technology stack	Non-MSA listed devices.
Work From Home Hardware Support (End Point Devices)	Yes, for listed MSA devices.	3rd party ISP connectivity support, home networks, and non-MSA listed devices.
PC Setup & Configuration	Yes, there is no setup fee for PCs purchased from GPK	On-boarding is charged for PCs not purchased from GPK
On-site Support	Yes, for listed MSA devices in head and branch offices using GPK's technology stack. On-site support at GPK's discretion	Work from the home sites, sites nominated as remote-only support sites and non-MSA listed sites.
Offboarding & Decommissioning	Yes, we'll remotely restore the device to its original factory settings, erasing all user data and settings using the built-in reset application. Hardware disposal remains the customer's responsibility. Please note that any on-site callouts for this service will be billed separately.	Secure Wipe (Billable Service): This service permanently erases all data, ensuring it's unrecoverable—ideal for decommissioning, resale, or repurposing devices with sensitive information. Disposal of the hardware remains the customer's responsibility, and any on-site callouts for this service will be billed separately.

Servers

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Proactive Monitoring & Alerting	Yes, for supported Windows servers (still supported by Microsoft) and monitored via GPK's RMM tool	EOL Windows Server versions or servers not monitored by GPK's RMM tool
Operating System Patch Management	Yes, using GPK's deployment tools for Windows Server OS still supported by Microsoft	Servers not using GPK's deployment tools or EOL Windows Server versions
Software Patch Management	Yes, for supported third-party server applications managed through GPK's tools	Unsupported or custom server software not managed by GPK
Backup Management	Yes, for supported backup systems like Veeam Cloud Connect	Backup systems not managed by GPK or unsupported third-party systems
Disaster Recovery Planning	Yes, disaster recovery planning is included in the standard GPK MSA.	
Disaster Recovery Testing	No, scoped and charged separately.	
Cybersecurity Incident Response	GPK's standard Cybersecurity Incident Response requires SentinelOne EDR and Vigilance Response subscriptions to manage and contain security incidents on endpoints and servers.	Advanced Incident Response is a premium, chargeable service not included in GPK's standard Cybersecurity Incident Response offering.
Email Security	Yes, requires Barracuda Email Protection solutions	Unsupported or third-party email security solutions
Web Application Firewalls (WAFs)	Yes, it requires Barracuda WAF or agreed-upon WAF devices.	Unsupported WAF solutions
On-premises Hardware Support (Servers)	Yes, for MSA listed supported hardware within GPK's technology stack, EOL	Unsupported or third-party hardware

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
	hardware is supported only if agreed upon and charged at a premium	
On-site Support	Yes, for listed MSA devices in head and branch offices. On-site support at GPK's discretion	

Network Infrastructure & Security

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Proactive Monitoring & Alerting	Yes, for network devices and security systems within GPK's technology stack. During the transition period, support will be provided for all named devices in the MSA agreement.	Unsupported or third-party network devices not agreed upon for management.
Operating System Patch Management (Network Devices)	Yes, for supported network and security devices managed by GPK. During the transition period, support will be provided for all named devices in the MSA agreement.	Devices not managed by GPK or not agreed upon for management.
Software Patch Management (Security/Network Software)	Yes, for supported network and security software within GPK's stack. During the transition period, support for named existing security/network software	Unsupported or custom software not managed by GPK or not agreed upon for management
Firewall & Network Security	Yes, for GPK-managed firewalls (requires Barracuda Firewalls). During the transition period, support for named existing firewalls	Firewalls not provided or managed by GPK and not agreed upon for management.
Incident Detection and Response	Yes, using standard alerting, logging, reporting, and GPK's tools and technologies for network devices	Network devices not managed by GPK or not agreed upon for management.
Threat Hunting and Analysis	Basic Threat Hunting and Analysis for customers utilising SentinelOne EDR with SentinelOne Vigilance Response.	Advanced Threat Hunting and Analysis is a premium, chargeable service not included in GPK's standard Cybersecurity Incident Response offering. Expert threat hunting available though SentinelOne WatchTower or

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
		SentinelOne WatchTower Pro managed threat hunting services
Security Audits and Assessments	Yes, basic standard monthly routine assessments	Full audits like ISO27001, Essential8, framework assessments (scoped and charged separately)
Vendor Management	Yes, coordination with supported network and security vendors within GPK's technology stack. During the transition period, support for agreed-upon vendors.	Unsupported third-party vendors not agreed upon for management.
On-premises Hardware Support	Yes, for supported hardware within GPK's technology stack. During the transition period, support will be provided for all named devices in the MSA agreement.	Unsupported or third-party hardware not agreed upon for management.
On-site Support	Yes, for general on-site visits when required, including support for all named devices in the MSA agreement.	Physical installation of network cabling or mounting devices (scoped and charged separately)
After-Hours Support	Yes, billed at after-hours rates for critical issues.	

Cybersecurity Incident Response

Endpoints and Servers

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Incident Detection and Response	Yes, for endpoints and servers using SentinelOne with Vigilance Response subscription	Devices without SentinelOne or Vigilance Response subscription; incidents on unsupported systems
Threat Hunting and Analysis	Yes, for customers utilising SentinelOne EDR with SentinelOne Vigilance Response and SentinalOne WatchTower or SentinelOne WatchTower Pro managed threat hunting services.	Devices without SentinelOne & SentinelOne WatchTower subscription; incidents on unsupported systems
Security Incident Reporting	Yes, for incidents detected on endpoints and servers within GPK's technology stack	Incidents on systems not within GPK's stack
Remediation and Recovery Assistance	Yes, we aid on supported endpoints and servers using GPK's tools and technologies. While we support various incidents, coverage may exclude wilful or malicious damage, issues arising from client actions against GPK's advice, and other situations beyond our control. Remediation and recovery assistance will utilise your most recent complete backup.	Systems not supported by GPK's tools or outside the MSA and technology stack.
Post-Incident Review and Recommendations	Yes, for incidents involving endpoints and servers within GPK's technology stack	Incidents on unsupported systems

Note: A subscription to SentinelOne Vigilance Response is necessary for advanced cybersecurity incident response services on endpoints and servers. A SentinelOne WatchTower or SentinelOne WatchTower Pro subscription is required to access managed threat hunting and analysis services.

Network Devices

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Incident Detection and Response	Using standard alerting, logging, reporting, and GPK's tools and technologies for GPK-managed network devices and customers using SentinelOne WatchTower or SentinelOne WatchTower Pro managed threat hunting services.	Network devices not managed by GPK or not agreed upon for management.
Threat Hunting and Analysis	Yes, for customers using SentinelOne WatchTower or SentinelOne WatchTower Pro managed threat hunting services.	Network devices not managed by GPK or not agreed upon for management.
Security Incident Reporting	Yes, for incidents detected on network devices within GPK's technology stack.	Incidents on devices not within GPK's stack or not agreed upon for management
Remediation and Recovery Assistance	Yes, we offer remediation and recovery assistance for network devices supported by GPK. Remediation and Recovery Assistance is based on restoring the most recent full-function backup and any necessary tweaks to the configuration.	Devices not supported by GPK's tools or outside the technology stack
Post-Incident Review and Recommendations	Yes, for incidents involving network devices within GPK's technology stack	Incidents on unsupported devices

Note: A subscription to SentinelOne Vigilance Response is necessary for advanced cybersecurity incident response services on endpoints and servers. A SentinelOne WatchTower or SentinelOne WatchTower Pro subscription is required to access managed threat hunting and analysis services.

Backup and Archiving Solutions

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Backup Management	Yes, for supported backup systems like Veeam Cloud Connect, Barracuda Cloud-to-Cloud Backup, and Azure Backup. During the transition period, support for agreed-upon existing backup and archiving solutions	Backup systems not managed by GPK or not agreed upon for management.
Disaster Recovery Planning	Yes, for systems within GPK's technology stack. During the transition period, support for agreed-upon existing backup and archiving solutions	Systems outside of GPK's technology stack and not agreed upon for management
Disaster Recovery Testing	No, it is scoped and charged separately. This is an optional MSA line item.	
Cybersecurity Incident Response (Backups)	Yes, for incidents involving backup systems within GPK's technology stack. During the transition period, support for agreed-upon existing backup and archiving solutions	Incidents on backup systems not managed by GPK or not agreed upon for management

Mobile Devices Enrolled in Intune (Managed with Microsoft Intune)

Service/Feature	**Included in GPK's MSA**	**Not Included in GPK's MSA**
Endpoint Management (Intune)	Yes, for Intune-enrolled and managed iOS and Android devices	Non-enrolled or unmanaged devices
Patch Management (Operating System - Intune)	Yes, for Intune-enrolled devices	Unmanaged or non-enrolled mobile devices
Patch Management (Software - Intune)	Yes, for Intune-managed mobile software	Unmanaged or unsupported mobile software
Remote Support	Yes, for Intune-enrolled and managed iOS and Android devices	Unmanaged or non-enrolled mobile devices
Cybersecurity Incident Response	Yes, for Intune-managed devices within GPK's technology stack	Devices not enrolled in Intune or not using GPK's recommended security solutions
Setup, Configuration, and Enrolment (Intune)	No, scoped and charged separately	

Note: Only applicable for customers who have deployed Intune in their environment.

Hardware & Software Deployment

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Software Deployment (Standard Packages)	Yes, for approved software via GPK's deployment tools (ImmyBot, Automate, Intune)	Custom application packaging and deployment not using GPK's tools.
Large Scale System Software Upgrades	No, it is scoped and charged separately.	
Large Hardware Upgrades and Replacements	No, it is scoped and charged separately.	
Project Management	No, it is scoped and charged separately.	

Hardware & Software Procurement

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Hardware and Software Procurement	Yes, for supported hardware and software within GPK's technology stack	Unsupported or third-party procurement outside of GPK's recommendations
License Purchases and Renewals	No, all license purchases and renewals (e.g., 3CX, SentinelOne, Microsoft) are charged separately.	
SentinelOne Licenses	No, they are charged separately.	
Warranty Management	Yes, for GPK-supplied hardware	Non-GPK procured hardware

Microsoft 365

Service/Feature	Included in GPK's MSA	Not Included in GPK's MSA
Backup & Restore (Microsoft 365)	Yes, requires Barracuda Cloud-to-Cloud Backup (licenses & deployment charged separately)	Non-Microsoft 365 backups or third-party tools
Microsoft 365 Licensing Management	Yes, assistance with license management; **license purchases and renewals are charged separately.**	Licenses purchased outside of GPK
Microsoft 365 Application Support	Yes, for standard Office 365 apps (Outlook, Word, Excel, etc.)	Non-Microsoft or custom applications
Microsoft Teams	Yes, basic support for Microsoft Teams	Advanced integration (e.g., phone system integration) is scoped and charged separately.
Microsoft 365 Security Management	Yes, for standard Microsoft 365 security settings within GPK's recommended configurations	Advanced security configurations (scoped and charged separately); configurations outside GPK's recommendations
Cybersecurity Incident Response	Yes, for incidents detected within Microsoft 365 when using GPK's recommended security solutions (e.g., Barracuda Email Protection)	Incidents involving third-party tools or configurations not recommended by GPK

Services Not Covered by GPK's MSA: When Additional Charges Apply

The following services are **not included** in the GPK MSA and will incur additional charges. These are considered project work or specialised services requiring separate scoping and billing.

Project/Service	**Description**
Hardware Purchases	Acquisition of new servers, networking equipment, workstations, or other hardware components (charged separately)
Software Purchases	New software licensing costs, including operating systems and specialised applications (charged separately)
Large-Scale System Upgrades	Large-Scale System Upgrades involve significant changes to an organisation’s IT infrastructure, such as migrating to a new server platform or upgrading enterprise software. These projects require detailed planning, substantial resources, and effective risk management. Key aspects include defining objectives, managing resources, mitigating risks, and ensuring thorough testing. Additionally, successful upgrades depend on effective change management and providing adequate training and support to users. These elements help ensure the upgrades are implemented smoothly and achieve their intended benefits.
Large-Scale System Deployments	Deployment of new systems, enterprise software, or hardware upgrades across the organisation
New Hardware Installations	Installation and configuration of new hardware for expansion or upgrades
Complex Change Requests	Complex Change Requests are customer-initiated modifications or enhancements that go beyond the predefined services outlined in the Master Service Agreement (MSA). These requests typically involve significant alterations to the existing infrastructure, integration of new technologies, or extensive custom development work. Due to their complexity and the resources required, they are not covered under the standard MSA and are billed separately, often requiring a detailed

Project/Service	Description
	assessment and approval process to ensure alignment with the customer's needs and GPK's capabilities.
Cloud Migrations	Migration to cloud platforms, including setup and configuration of cloud resources not within GPK's technology stack
System Migrations	Moving from one software platform or system to another (e.g., legacy to modern applications)
Custom Development	Bespoke software development or customisation for specific business needs
Infrastructure Design	Planning and designing new IT infrastructure, such as setting up a new office
Security Audits and Compliance Remediation Plans	Security assessments and remediation plans to meet standards like Essential8, ISO27001 and PCI compliance, including audits
Security Audits and Penetration Testing	Comprehensive security assessments, including penetration testing and detailed audits
Training	Training sessions beyond basic user orientation on standard systems
Network Cabling and Mounting	Physical installation of network cabling or mounting devices (scoped and charged separately)
Disaster Recovery Testing	Full disaster recovery testing exercises, including simulations and reporting
Setup, Configuration, and Enrolment (Intune)	Initial setup and enrolment of mobile devices into Microsoft Intune
Phone Setup & Configuration (3CX)	Setup and configuration of new phones or changes to existing configurations not purchased from GPK
MS Teams Integration with 3CX	Integration services between Microsoft Teams and 3CX phone systems

Project/Service	**Description**
Advanced Security Configurations (Microsoft 365)	Implementing advanced security features like Conditional Access, Identity Protection

Additional Billing Considerations

- **Technology Stack Compliance and Transition Support**: Full coverage under the MSA is contingent upon the customer's use of GPK's recommended technology stack. During the transition period, GPK will support agreed-upon existing firewalls, switches, wireless access points, backup and archiving solutions, and EDR/XDR solutions. Support limitations and additional charges may apply for systems not agreed upon for management.
- **License Purchases and Renewals**: All license purchases and renewals (e.g., SentinelOne, Microsoft 365, 3CX) are charged separately.
- **Hardware Purchases**: Acquisition of new hardware components is charged separately.
- **SentinelOne Vigilance Response Subscription**: A SentinelOne Vigilance Response subscription is required for Threat Hunting, analysis, incident Detection, and Response for endpoints and servers.
- **Network Devices Coverage**: For network devices, GPK utilises standard alerting, logging, reporting, and its own tools and technologies for Incident Detection and Response and Threat Hunting and Analysis. SentinelOne Vigilance Response does not cover network devices.
- **After-Hours Support**: Support requested outside standard business hours is charged at after-hours rates.
- **Replacement Parts & Materials**: Costs for parts or materials required for repairs or upgrades are charged independently.
- **Third-Party Services**: Services from third-party providers not covered under existing agreements will incur additional charges upon approval.
- **Extended Training & Workshops**: In-depth training sessions beyond basic user training are charged separately.

- **Requests for a Senior Engineer:** Requests for a senior engineer outside of the normal escalation process (i.e., a customer insists on a specific or senior resource when a ticket hasn't gone through the standard triage/escalation process).
- **Requests for Specific Actions:** Requests for a specific action (e.g., Windows re-install) where the ticket has not gone through the standard triage/escalation process or wasn't deemed necessary by a GPK technician (e.g., customer wants a PC wiped and re-built to hand over to a new staff member where a simple profile cleanup would normally suffice).

GPK Patch Management Process Overview

As a Managed Service Provider (MSP), GPK is dedicated to protecting our clients' IT environments through a comprehensive patch management process. We proactively manage software updates using ConnectWise Automate and other tools to automate deployment and reduce manual errors. Our approach focuses on enhancing security, ensuring stability, deploying only approved patches, and maximising system efficiency.

We implement a strategic lag before deploying patches to production environments. During this period, we thoroughly test all patches in a controlled setting to ensure they are compatible with your existing systems and do not introduce unforeseen problems. Only after a patch has passed our testing and approval process do we deploy it to your environment. By deploying only approved patches, we maintain the stability and reliability of your IT infrastructure while safeguarding against potential vulnerabilities.

To minimise any impact on your business operations, we schedule patch deployments at 3 a.m. This timing ensures that updates occur during off-peak hours when system usage is low, reducing the likelihood of disruptions to your users. We strongly encourage you to leave your systems powered on overnight to avoid missing these critical patching windows. Keeping your devices on allows us to perform necessary maintenance without interrupting your workflow, helping to keep your environment secure and up to date.

Manual Intervention for Patch Updates

While our automated patch management system handles most updates efficiently, there are certain circumstances where manual intervention may be necessary to ensure your systems are fully patched:

- **Offline or Powered-Off Devices**: If a system is turned off or disconnected from the network during the scheduled patching window, it may miss critical updates. In such cases, manual intervention is required to bring the system up to date once it's back online.
- **Patch Conflicts or Errors**: Some patches may fail to install automatically due to software conflicts, outdated system components, or insufficient resources. Our team will manually troubleshoot and resolve these issues to ensure the patch is successfully applied.
- **Specialised Software Updates**: Systems running specialised or legacy applications may require manual patching because automatic updates could disrupt functionality. We carefully apply these patches manually to maintain system integrity.
- **Critical Security Vulnerabilities**: In the event of a high-priority security threat, immediate manual intervention may be needed to deploy patches outside the regular schedule to protect your systems promptly.
- **Hardware Compatibility Issues**: Updates that affect hardware drivers or firmware might need manual verification and installation to prevent hardware malfunctions or performance issues.

In these situations, our experienced team will coordinate with you to perform the necessary manual updates with minimal disruption to your operations. We prioritise transparent communication to keep you informed about the steps we're taking to secure your environment.

Scope of Patching Services

Our standard Master Services Agreement (MSA) includes patching for Windows Desktop and Server Operating Systems, Microsoft 365, and software patching related to GPK's technology stack. This ensures that your core systems and applications are kept up to date with the latest security updates and performance improvements.

For any other non-operating system patching, such as updates for specific third-party software packages, we can include these services if they are added to your MSA as approved line-of-business software applications. By explicitly including these applications in your agreement, we can tailor our patch management services to cover the software critical to your business operations.

Don't hesitate to contact us to discuss any additional software patching needs you may have. We are committed to customising our services to meet your unique requirements and ensuring that all aspects of your IT environment are securely maintained.

Fair Usage Policy

GPK is committed to providing excellent service under fair usage terms. Services included in the MSA cover standard operational needs. Activities outside normal usage patterns, requiring excessive resources, or involving unsupported technologies not agreed upon for management may incur additional charges after consultation with the customer.

Summary

This matrix clarifies what is included in the GPK MSA and outlines scenarios where additional fees may apply. Our aim is to ensure transparency and fairness. For services not explicitly mentioned or if you have systems outside GPK's technology stack, please consult your GPK account manager to agree upon management during the transition period and to understand any support limitations or potential additional costs.