

Your IT partner in a changing world

Service Definition Document: Microsoft Intune Services for Secure Endpoint Management & Compliance

G-Cloud | Service Definition and Pricing Document



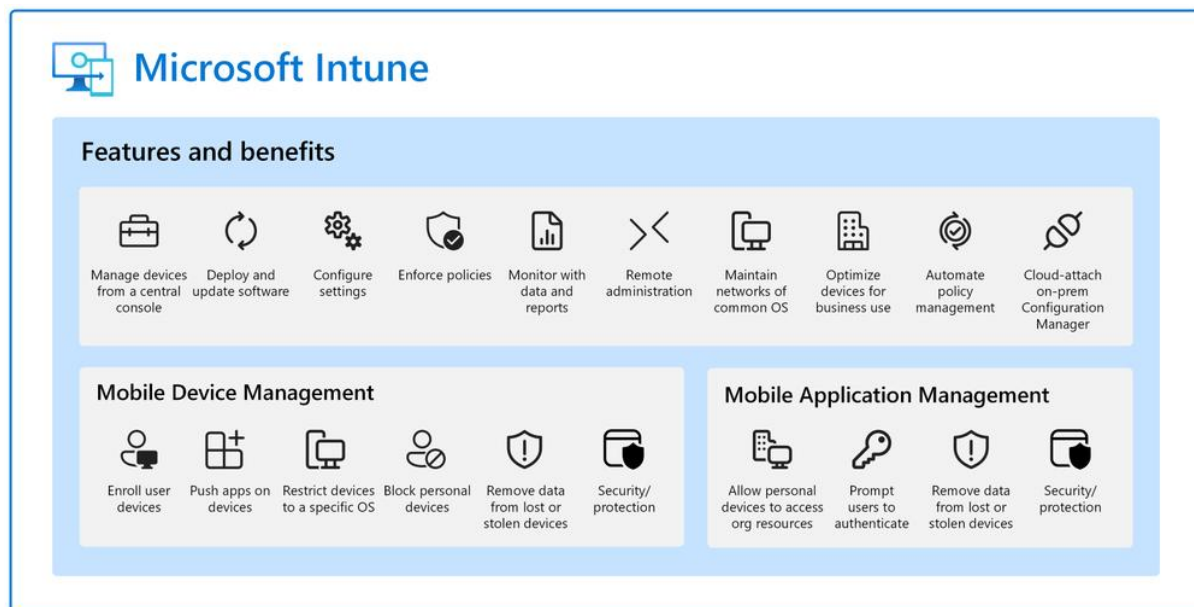
Contents

Executive Summary	2
Services Overview	3
Security and Compliance by Design	3
Cost Savings and Operational Efficiency	3
Risk Mitigation	4
Digital Transformation	4
Remote and Hybrid Workforce	4
Microsoft Intune: Fixed Price Proof of Concept	5
Microsoft Intune: Implementation Service.....	7
Microsoft Intune: Health Check and Evergreen Service	9
Microsoft Intune: Managed Service	10
Service Scope	10
Service Assurance and Governance	10
Flexible Engagement Model	10
Service Levels and Performance Management	11
Exit and Knowledge Transfer	12
Pricing Information	13
Exit Costs	13
Invoicing	13
About APPtechnology	14
Contact Details.....	14

Executive Summary

Our services enable government organisations to securely modernise and operate their endpoint environments using Microsoft Intune, while maintaining strong governance, cost control, and operational assurance.

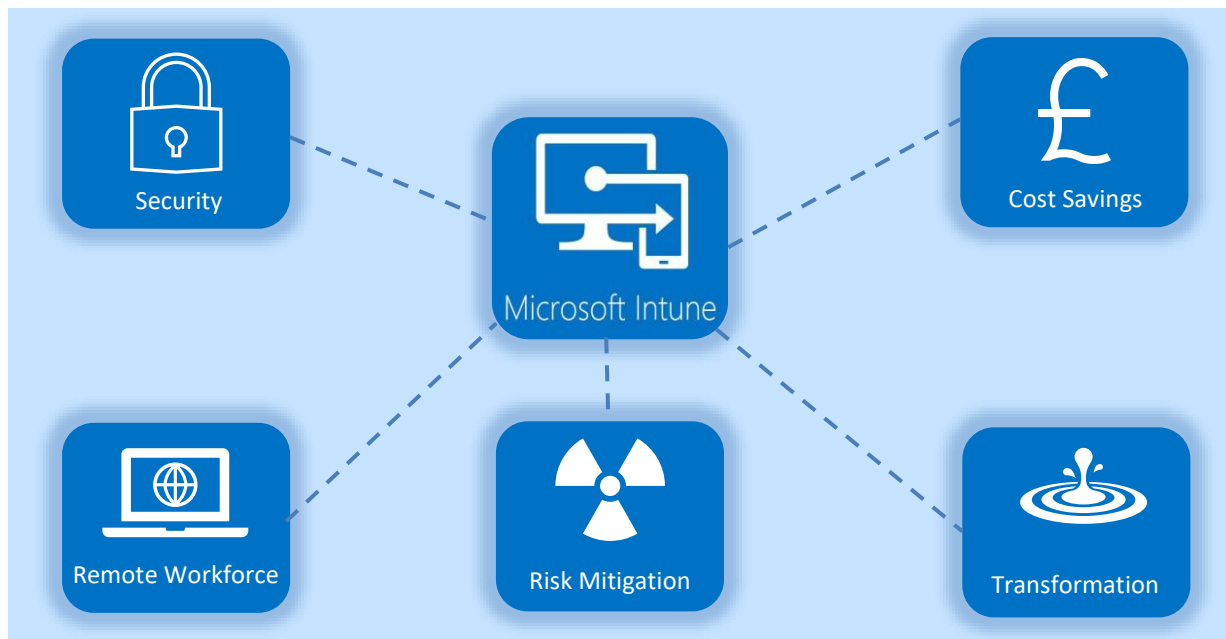
- Services are structured to support governance, audit, and internal approval processes, with clear documentation, defined service boundaries, and UK-based service management.
- Supports co-sourced or fully managed delivery, enabling organisations to retain strategic control while reducing operational burden.
- Fixed-price assurance options, phased implementation, and controlled adoption of platform changes help de-risk modern workplace transformation.
- Evergreen health checks, service reporting, and knowledge transfer ensure the service remains supportable over time and avoids vendor lock-in.



APPTechnology brings proven experience delivering secure endpoint management services across central and local government and NHS environments. Our services are delivered and governed from the UK, with a strong focus on assurance, documentation, and operational resilience. We work flexibly with customer teams, supporting co-sourced or fully managed models, and place particular emphasis on reducing delivery risk through fixed-price assurance, clear service boundaries, and sustainable handover. This approach enables government organisations to modernise with confidence while retaining appropriate control and oversight.

Services Overview

APPtechnology partners with government organisations to securely migrate, deploy, and operate Microsoft Intune, enabling a modern, compliant, and cost-effective approach to endpoint management. Our services range from fixed-price proofs of concept through to fully managed, evergreen Intune operations.



Security and Compliance by Design

Intune provides a security-first, cloud-native platform that supports stringent government security and compliance requirements. Centralised policy enforcement, device compliance controls, conditional access, and data protection capabilities ensure sensitive information remains protected across all endpoints—whether government-owned or BYOD—while supporting auditability and regulatory obligations.

Cost Savings and Operational Efficiency

By replacing fragmented on-premises tooling with a single cloud-based service, Intune reduces infrastructure overheads, licensing complexity, and support effort. Automated device provisioning, policy deployment, and patching streamline operations, freeing IT teams to focus on higher-value initiatives while delivering measurable cost efficiencies.

Risk Mitigation

Migrating from ageing endpoint management platforms reduces security vulnerabilities, technical debt, and reliance on unsupported systems. Intune provides continuous updates and modern security controls, lowering the risk profile associated with legacy device management solutions.

Digital Transformation

Intune aligns strongly with government digital transformation strategies by supporting cloud adoption, zero-trust security models, and modern workplace initiatives. Its native integration with Azure and Microsoft 365 enables a scalable, standards-based approach to modern service delivery across agencies.

Remote and Hybrid Workforce

Intune empowers a secure, productive workforce regardless of location—an essential capability in the post-pandemic operating model. Staff can safely access government systems from Windows, macOS, iOS, and Android devices, with consistent security controls applied across office-based, remote, and hybrid working environments.

APPtechnology provides end-to-end Intune consultancy, including architecture design, security configuration, deployment, project and programme management, and ongoing managed services—ensuring your Intune environment remains secure, compliant, and continuously optimised.

Microsoft Intune: Fixed Price Proof of Concept

A low-risk, fixed-price engagement designed specifically to help government organisations validate, assure, and de-risk the adoption of Microsoft Intune and Windows Autopilot before committing to full-scale rollout.

This PoC provides clear evidence-based outcomes, enabling informed decision-making aligned to government security, compliance, and digital transformation objectives.

- Confirm whether Intune and Autopilot can meet your security, compliance, operational, and workforce requirements, including support for government-owned and BYOD devices.
- Review existing device build, application delivery, and patch management processes to identify risks, inefficiencies, and legacy constraints.
- Identify gaps between current practices and modern, policy-driven endpoint management aligned to government security expectations.
- Establish a secure Model Office configured to reflect your environment, allowing stakeholders to safely trial modern workplace capabilities without impacting production systems.
- Demonstrate real-world scenarios relevant to government, including device provisioning, policy enforcement, application deployment, and secure remote access.
- Provides a pragmatic, phased roadmap outlining the steps, dependencies, and effort required to move from PoC to a fully managed production environment.

Ref.	Deliverables	Acceptance Criteria
D01	Pre-engagement confirmation of pre-requisites • Conference call in advance of engagement to walk through the Customer pre-requisites and identify outstanding requirements.	APPtechnology account manager and Customer Project Management
D02	Review of current processes and features used. • Build process. • Patch process. • Update process. • Application Deployment process.	APPtechnology Consultant / Customer Operational Team
D03	Gap analysis and opportunity review for moving to Autopilot and Intune;	APPtechnology Consultant

	• Build from current to Autopilot / Intune • Patching and updates from current to Intune • Application deployment from current to Intune	
D04	Configure Intune and Autopilot in Proof of Concept • Setup Autopilot process • Setup patching and update management via Intune • Setup application deployment via Intune	APPtechnology Consultant / Customer Operational Team
D05	Demonstrate Intune and Autopilot Proof of Concept • Demonstration on two common devices. • Demonstrate Autopilot process. • Demonstrate patching and windows update options via Intune. • Demonstrate a sample application deployment.	APPtechnology account manager and Customer Project Management
D06	Create Next Steps Recommendations • Creation of next steps presentation. • Inclusion of key engagement highlights. • Hosting of presentation for stakeholders. • Engagement closure.	APPtechnology account manager and Customer Project Management

Microsoft Intune: Implementation Service

APPtechnology delivers a structured, security-focused implementation of Microsoft Intune, enabling government organisations to centrally manage operating systems, applications, patching, and security controls across their entire endpoint estate.

Our implementation approach is designed to meet government expectations for governance, risk management, and operational readiness, while supporting modern, internet-facing service delivery for remote and hybrid workforces. Cloud-based distribution reduces reliance on on-premises infrastructure and minimises network bandwidth consumption for operating system and large application updates.

- Structured workshops to capture business, security, compliance, and operational requirements, ensuring alignment with government policies and standards.
- Development of a formal High-Level Design (HLD) covering architecture, security controls, device management approach, and integration points, suitable for internal governance and assurance approval.
- Configuration of endpoint management policies to support consistent security posture, controlled application delivery, and automated patching across supported device platforms.
- Comprehensive operational documentation to support day-to-day management, incident response, and ongoing service operation.
- Documentation covering handover to operations, alongside defined processes for future upgrades, policy changes, and platform evolution—supporting long-term sustainability and reduced operational risk.

Ref.	Deliverables	Acceptance Criteria
D01	Pre-engagement confirmation of pre-requisites • Conference call in advance of engagement to walk through the Customer pre-requisites and identify outstanding requirements.	APPtechnology account manager and Customer Project Management
D02	Review of current processes and features used. • Build process. • Patch process. • Update process. • Application Deployment process.	APPtechnology Consultant / Customer Operational Team
D03	Architecture Design • High Level Design	APPtechnology Consultant

	• Low Level Design	
D04	Implementation and configuration of Microsoft Intune • Setup patching and update management via Intune • Setup application deployment via Intune	APPtechnology Consultant
D05	Transition to BAU • Training • Documentation Handover • Go-Live	APPtechnology account manager and Customer Project Management

Pricing and deliverables increase based on the inclusion of Autopilot and / or SCCM upgrades / cloud migrations, along with other optional services such as OS image build, application packaging or distribution via Intune

Microsoft Intune: Health Check and Evergreen Service

APPtechnology's Health Check Service provides government organisations with ongoing assurance that their Microsoft Intune environment remains secure, compliant, and aligned with both organisational policy and evolving Microsoft capabilities.

Through scheduled consultant-led reviews, we assess the configuration, usage, and operational effectiveness of your Intune environment, ensuring that security controls are consistently applied and that emerging platform enhancements are evaluated in a controlled and risk-aware manner.

- Review of device compliance policies, configuration baselines, and access controls to help maintain alignment with government security and audit requirements.
- Assessment of Intune tenant configuration, policy sprawl, device coverage, and operational practices to identify misconfigurations, inefficiencies, or emerging risks.
- Analysis of relevant Microsoft Intune product updates, with clear guidance on which enhancements are suitable for adoption within a government environment.
- Presentation of findings and recommendations, followed by agreed and governed implementation of approved improvements to minimise operational risk.
- Delivery of a concise Health Check report suitable for governance, audit, and internal assurance stakeholders.

Ref.	Deliverables	Acceptance Criteria
D01	Review of issues of conflicts in Intune configuration	Supply of documentation
D02	Mini Health check of previous periods internal activity levels, incidents and escalated issues	Workshop delivery
D03	Gap analysis and opportunity review for moving to Autopilot and in presentation of recent product advances in Intune or Intune product suite.	Presentation delivery
D04	Recommendations of product advances relevant to your environment	Document delivery
D05	Agreement on which product advances are to be implemented, and their approach (Model Office, Dev, Pilot or Production)	Workshop delivery
D06	Implementation as per agreed plan	Implementation Signoff
D07	Schedule next review dates	Document delivery

Microsoft Intune: Managed Service

APPtechnology provides a secure, UK-based managed service for the ongoing administration and operation of your Microsoft Intune and Microsoft Endpoint Configuration Manager environments hosted on Microsoft Azure.

The service is designed to support government organisations seeking operational resilience, reduced risk, and assured service delivery, while maintaining appropriate levels of internal oversight and control.

Service Scope

- Day-to-day administration of device management services, including policy management, configuration changes, and operational support.
- Controlled application packaging, deployment, and patch management to maintain security posture and service stability.
- Management of Windows 10/11 servicing cadences, feature updates, and Operating System Deployment (OSD) activities.
- Planned SCCM infrastructure upgrades and lifecycle management to reduce technical debt and maintain platform supportability.
- Proactive monitoring of system health and performance to identify issues early and support service continuity.

Service Assurance and Governance

APPtechnology delivers the Managed Service under a defined governance model aligned to public sector expectations. This includes clear service ownership, agreed escalation paths, change control processes, and regular service reporting.

Governance activities ensure that operational delivery remains aligned with organisational security policies, service priorities, and risk management frameworks, while enabling transparent oversight by customer service owners.

Flexible Engagement Model

- Entry-level service starting from 40 support hours per month, suitable for low-level administration and operational support.

- Ability to scale through to a fully outsourced management model for cloud-based SCCM and Intune, with APPtechnology taking end-to-end operational responsibility as required.
- Clearly defined service boundaries allow organisations to retain strategic control while delegating operational workload—freeing internal teams to focus on frontline and mission-critical delivery.

APPtechnology supports both co-sourced and fully managed operating models. Customers retain strategic control, policy authority, and security ownership, while APPtechnology assumes responsibility for agreed operational activities. Roles and responsibilities are clearly defined to support accountability and effective collaboration.

Service Levels and Performance Management

Service levels are agreed during onboarding and tailored to organisational requirements. Typical measures include:

- Patch and Update Compliance aligned to information security policy
- Incident Response and Resolution Targets based on priority and impact
- Windows 10/11 Servicing Cadence Management, including controlled pilot and release processes
- Service Availability and Operational Health Monitoring

Performance is reviewed through regular reporting and service reviews, supporting continuous improvement and assurance.

	Acceptance Criteria
On demand application deployment	SLA based against user expectations
Patch release management	SLA based on your InfoSec requirements
Windows 10/11 Servicing	SLA based pilot and release service for new features
Dashboard service reporting	Or integrated into your service desk
SCCM Upgrades	Ensuring that your SCCM version can support current and future Windows 10/11 releases
Integration with your internal helpdesk solution	Users can manage the status and priority of their call
Active Directory creation, deletion and updating objects	Collections, Applications, Patching, Security Updates, OS deployment
Remote Client Installations	On demand
Troubleshooting of Infrastructure and client issues	As required
Intune management tasks	Alerts, client compliance, health and license usage

SCCM Monitoring tasks	Management points, distribution points, software update points, database servers
Intune Monitoring tasks	
SCCM reporting	Deployments, security updates, OSD, client health, site server, customer reports
Intune reporting	Updates, detected software, inventory, mobile devices, certificate compliance, device history

Our outsourced model pricing is dependent upon the size of your environment, the complexity of the component tasks that you would like to be provided in the outsourced model, and the SLA based timescales agreed for each component service. Our cost-free presales engagement will define your requirements and provide an annual cost that covers all components that you require.

Exit and Knowledge Transfer

The service is designed to support orderly transition at contract end. Documentation, configuration knowledge, and operational procedures are maintained throughout delivery, enabling smooth handover to an alternative supplier or in-house team with no service lock-in.

Pricing Information

Pricing depends upon the detailed technical solution required that matches your Microsoft Endpoint Manager requirements and the size of your current estate. Range examples below are based on the SFIA rates and differing levels of day rate requirements.

	Cost	Notes
Microsoft Endpoint Manager Price Proof of Concept	£6,999 - £10,999	Based on size of environment and exact requirements.
Microsoft Endpoint Manager Implementation Service	£10,999 - £18,999	Based on size of environment and exact requirements.
Microsoft Endpoint Manager Health Check and Evergreen Service	£18,500 - £39,000	Based on size of environment and exact requirements.

Standard Consultancy Pricing

	Strategy and Architecture	Business Change	Solution Development and Implementation	Service Management	Procurement and Management Support	Client Interface
1. Follow	£450	£450	£450	£400	£450	£450
2. Assist	£600	£600	£600	£550	£600	£600
3. Apply	£725	£725	£725	£675	£725	£725
4. Enable	£800	£800	£800	£725	£800	£800
5. Ensure/Advise	£950	£950	£950	£800	£950	£1150
6. Initiate/Influence	£1100	£1100	£1100	£900	£1100	£1100
7. Set Strategy and Inspire	£1250	£1250	£1250	£1000	£1250	£1250

Exit Costs

Provided that the services terminate at the end of an agreed term, in line with the terms and conditions, there are no specific exit costs.

Invoicing

Monthly in Staged invoices based on Statement of Work Delivery.

Monthly in arrears for each agreed SoW phase.

About APPtechnology

APPtechnology provide application lifecycle solutions into Enterprises across Government, Financial, Retail and Banking sectors. Our combination of software and professional services lowering the costs and time to make applications available to end users. We're based in London so we're close to our clients and offer a sensible balance of on-site and off-site capabilities.

Contact Details

Question related to minimum order values, design and implementation costs and other technical questions related to the Service should be addressed to:

operations@apptechnology.co.uk

Or alternatively contact Martin Sweeney at:

28th Floor, the Gherkin
30 St Mary Axe
City of London
EC3A 8BF

Tel: +44 207 469 4053

About APPtechnology

APPtechnology is a leader in digital transformation services, covering project and BAU delivery for large organisations Globally.

We supply flexible teams specialising in Modern Workspace delivery, covering Endpoint Management, Security, Data protection, End User Experience management and Technology migrations.

Entirely managed from the UK, we bring experienced governance to all statement of work based delivery, incorporating measurable performance metrics and results analysis in our regular reporting. Where qualified resource supply only is requested we provide models for inside and outside of IR35 payroll, as appropriate to the role and delivery method.

We supply G-Cloud services to the largest (96,000 users) and the smallest local and central Government departments and NHS accounts.

