infotrust

SECURE YOUR FUTURE.

PREVENTATIVE MAINTENANCE POLICY – MANAGED ENDPOINTS

Infotrust Managed Technology

Date: 10/04/2026

Version 1.1

Document Change Control

Document	**Preventative Maintenance Policy – Managed Endpoints**	**State**	**Final**

Copyright Statement

Contents

1. Executive Summary 4
   1.1. Policy Purpose 4
   1.2. Endpoint Scope 4
   1.3. Out of Scope Endpoints 4
   1.4. Definitions 5
2. Preventative Maintenance Management 6
   2.1. Patch and Update Scope 6
   2.2. Patch Cadence 7
   2.3. Tools Used 7
   2.4. Pre-Patch Requirements 9
   2.5. Backup and Snapshot Rules 9
   2.6. Edge Cases and Exceptions 9
   2.7. Sequencing Rules 10
   2.8. Rollback Method 11
   2.9. Compliance and Metrics 12
3. Exception and Risk Acceptance 13
   3.1. Exception Requests 13
   3.2. Risk Assessment 13
   3.3. Risk Register Management 13
   3.4. Customer Risk Acceptance and Waiver 14
   3.5. Exception Review Cycle 14
   3.6. Exception Limits 14
   3.7. Exception Closure and Reinstatement 15
4. Responsibilities 16
   4.1. Infotrust Managed Technology 16
   4.2. Customers 16
   4.3. Third Party Vendors 17

1. Executive Summary

This Preventative Maintenance Policy defines how Infotrust Managed Technology manages patching and updates across all managed endpoints within its customer base. It establishes the standards, responsibilities, and governance requirements that ensure managed endpoints remain secure, stable, and operating on vendor-supported software.

This policy applies to Infotrust engineering and service delivery staff responsible for endpoint management, and to customers whose endpoints are under an Infotrust managed services agreement. It should be read in conjunction with each customer's managed services agreement, which defines contracted service levels and any customer-specific arrangements.

1.1. Policy Purpose

The purpose of this policy is to define the preventative maintenance standards applied to all managed endpoints under Infotrust Managed Technology's management. It sets the requirements for patching, updates, compliance, and reporting.

The policy exists to ensure endpoint environments remain protected, consistent in their operational behaviour, and maintained in accordance with vendor support requirements. It also provides customers with clear visibility of what Infotrust will do, when, and under what conditions.

1.2. Endpoint Scope

This policy applies to all endpoints under a managed services agreement with Infotrust, including:

- Desktop computers (physical and virtual desktop infrastructure)
- Laptop computers
- Tablet devices running Windows OS
- macOS devices (Apple MacBooks, iMacs, Mac Mini)

1.3. Out of Scope Endpoints

The following endpoints are excluded from this policy:

- Chrome OS devices
- Mobile devices (iOS, Android)
- Linux Endpoints
- Specialised endpoints as defined by customer (e.g., point-of-sale systems, kiosks, industrial control terminals, medical devices)
- Systems not onboarded into Infotrust's Management Platform
- Systems running unsupported Windows or macOS versions
- Offline or unused workstation devices
- Workstation devices where an underlying 3rd party vendor issue limits patching capabilities

Customers must explicitly identify any endpoints requiring exclusion from patching via their Technical Delivery Manager. Excluded endpoints are added to the Risk Register.

1.4. Definitions

For the purposes of this policy, the following definitions apply:

Term	Definition
Managed Endpoint	Any workstation, laptop, or tablet under active management by Infotrust as defined in a managed services agreement and onboarded to Infotrust management tooling.
Preventative Maintenance	Scheduled activities including patching, updates, upgrades, and configuration changes intended to maintain system security, stability, and supportability.
Patch	A vendor-supplied software update that addresses bugs, security vulnerabilities, or functional improvements.
Standard Update	A vendor-supplied, non-security patch applied on the regular automated patching cadence. These address functionality improvements, minor bugs, and general software maintenance.
Critical Update	A patch or update rated as critical or high severity by the vendor or recognised security advisories (e.g., ASD, CISA, vendor bulletins).
Feature Update	A major operating system version upgrade (e.g., Windows 10 to Windows 11) managed under a separate cadence and requiring customer approval.
Infotrust Management Platform	The platform used by Infotrust to deploy, monitor, and report on endpoint patching activity.
Blackout Period	A customer-requested timeframe during which patching and reboot enforcement are suspended due to business requirements.
Compliance State	The patch status of an endpoint: • **Compliant** - all applicable patches applied • **Non-Compliant** - patch deadlines missed without approved implementation • **Exception Approved** - operating outside policy with documented risk acceptance.
Rollback	The process of reverting an endpoint to its pre-patch state following a failed or problematic update.
Risk Acceptance Waiver	A signed customer document acknowledging the risks associated with operating an endpoint outside policy requirements.
TDM (Technical Delivery Manager)	The Infotrust contact responsible for customer relationship management, exception oversight, and escalation within the managed services engagement.

2. Preventative Maintenance Management

2.1. Patch and Update Scope

Operating System Patches

Any Supported Operating System security updates, critical updates, and cumulative updates for supported Windows or macOS versions as per the standard patching cadence. Supported versions include any Windows operating system for which Microsoft is actively releasing security patches and updates (currently Windows 10 and Windows 11).

Feature updates (for e.g. major version upgrades such as Windows 10 to Windows 11, or Windows 11 22H2 to 23H2) are managed via a separate patching cadence and require separate change management and customer approval.

Third-Party Application Updates

The following commonly deployed third-party applications are included in the standard patching scope where present on managed endpoints:

Application Category	Applications Covered
Productivity	Microsoft Office, OneDrive
Web Browers	Google Chrome, Mozilla Firefox, Microsoft Edge
PDF Readers	Adobe Acrobat Reader, Adobe Acrobat Pro
Runtime Environments	.NET Desktop Runtime, C++
Collaboration Tools	Zoom, Slack, Webex
Media Players	VLC Media Player

Third-party application patching is provided as a value-add service outside of contracted SLA. It is performed on a best commercial endeavour basis to improve the security posture and resilience of managed endpoints.

Patching of the above applications is subject to Infotrust's Management Platform capability. Some applications update via vendor-controlled mechanisms and cannot be patched through Infotrust's Management Platform.

Line-of-business applications and custom software are excluded unless explicitly included and listed in the customer's managed services agreement.

This service does not constitute Vulnerability Management. Application updates are applied as made available by vendors and are not governed by vulnerability severity or risk prioritisation frameworks.

Driver and Firmware Updates

Driver updates are included where available via Microsoft Update Services. Firmware updates are excluded from standard patching cycles and require individual assessment and customer approval.

2.2. Patch Cadence

Standard Patching Cycle

Daily Patching cycle operates as follows:

Step	Activity	Detail
1	Patch deployment	Daily as released, from 4:00AM as devices come online
2	Reboot notification (1 of 4)	First notification issued immediately upon patch deployment
3	Reboot notification (2 of 4)	Issued 4 hours after deployment
4	Reboot notification (3 of 4)	Issued 8 hours after deployment
5	Forced reboot notification (4 of 4)	12 hours after deployment (5 minute warning issued before reboot commences)

2.3. Tools Used

Primary Management Platform

Endpoint patch management across all in-scope endpoints is delivered via Infotrust's management platform. The platform provides automated patch deployment, compliance monitoring, reboot management, and agent-based control of endpoints regardless of physical location.

The agent-based architecture ensures Infotrust maintains visibility and control over endpoints whether in the office, at home, or travelling, supporting modern hybrid work environments while maintaining consistent security posture.

Onboarding Requirements

Endpoints must meet the following requirements before preventative maintenance services can be delivered:

- Infotrust's Management Platform agent is installed and functioning
- Appropriate administrative access is available to Infotrust

Endpoints that do not meet these requirements are ineligible for preventative maintenance until resolved. Infotrust will notify the customer's Technical Delivery Manager of any endpoints failing to meet onboarding requirements.

Patch Approval Process

All in-scope patches are pre-approved for deployment, enabling rapid response to security threats without manual review bottlenecks. Infotrust maintains patch approval policies that automatically approve:

- All security updates and critical updates for supported operating system versions
- Updates for third-party applications listed in section 2.1.

Patches classified as "Optional" or "Feature Updates" are excluded from automatic approval and require manual assessment before deployment, as these carry a different risk profile and may introduce significant system changes.

Monitoring & Alerting

The management platform provides real-time monitoring across patch deployment status, endpoint reboot status, failed installations, offline devices, and compliance percentage per customer.

Alerts are generated automatically for failed deployments, persistent non-compliance, and devices requiring manual intervention which enables the service desk to resolve issues proactively rather than waiting on scheduled reporting cycles.

Manual Patching

Manual patching outside Infotrust's Management Platform is exception-based only. Where manual patching is required, it must be:

- Documented with justification for why automated deployment is not feasible
- Approved by the Technical Operations Manager

Manual patching outside Infotrust's Management Platform may incur additional charges. Customers will be advised prior to work commencing.

2.4. Pre-Patch Requirements

Customer prerequisites

- No outstanding action on a customer's behalf is preventing successful patching.
- Customer has communicated the patching and reboot policy to end users
- Customers using endpoints in a server-like capacity (e.g. file hosting, application hosting, or hosting a critical line-of-business application) must notify their Infotrust Account Manager prior to enrolment. Customers wishing to exclude these devices from standard patching must complete a Risk Acceptance Waiver acknowledging the associated security risk. An alternate patch schedule will be agreed for these circumstances.

2.5. Backup and Snapshot Rules

Standard Endpoints

Infotrust does not perform pre-patch backups or snapshots of individual endpoints as part of standard preventative maintenance. This reflects the nature of endpoint computing where local data should not be mission-critical, and data protection mechanisms should exist independently of patching activities.

Endpoint data protection relies on two primary mechanisms:

- **Infotrust Backup Service (where enrolled)** - Provides protection for OneDrive and associated cloud data as part of the customer's managed services agreement
- **Customer responsibility -** Customers requiring additional data protection (such as endpoint snapshots or image-based backups) should notify their Account Manager. Infotrust can assess and provide a suitable solution outside the scope of this policy.

2.6. Edge Cases and Exceptions

The standard patching and reboot cycle is designed to handle the majority of endpoint scenarios. The following defines expected system behaviour where endpoints or user circumstances fall outside the standard path.

Scenario	Behaviour
Device offline at patch deployment	Patches deploy at next connection. The 12-hour reboot enforcement window starts from the point of successful patch installation, not the original deployment time.
User on extended leave	Device flagged as non-compliant in reporting. The 12-hour enforcement window triggers on next login following patch installation.

Patch installation failure	Reboot enforcement does not trigger. Device is flagged for failed deployment and reviewed by the service desk. Redeployment is attempted at the next available opportunity.
Laptop on battery at enforcement time	Forced reboot is deferred until AC power is connected or the user logs in, whichever occurs first. Device is flagged as non-compliant until resolved.
Shared or hot desk workstations	Enforcement applies at the device level regardless of which user is logged in at the time of enforcement.
Device in presentation or kiosk mode	Forced reboot is deferred until the device exits presentation or kiosk mode. Device is flagged as non-compliant if the enforcement window lapses.
Active blackout period	Patching and reboot enforcement are deferred to the next available cycle. Customers are responsible for notifying Infotrust of blackout periods in advance.
Patch requires multiple reboots	Some updates require more than one restart to complete installation. Where this occurs, the reboot cycle repeats until the patch is fully applied. The device remains flagged as pending until all reboots are complete.
Persistent non-compliance	Devices consistently failing to reach a compliant state are escalated to the customer's Technical Delivery Manager. Infotrust will work with the customer to identify and resolve the underlying cause.
Known issues with the patch	Where a known issue is identified with a patch, deployment is paused pending vendor resolution or Infotrust assessment. Affected endpoints are flagged as pending in reporting and the customer's TDM is notified.
Metered Connections (Mobile Data)	Patch deployment is deferred until a non-metered connection is detected. The endpoint is flagged as pending in compliance reporting until patching completes successfully.

Scenarios not covered by this table will be assessed by the service desk on a case-by-case basis and escalated to the Technical Delivery Manager where required. Customers with known edge cases that fall outside standard behaviour should notify their Account Manager prior to enrolment to ensure appropriate handling is documented before the policy takes effect.

2.7. Sequencing Rules

Patches deploy to all in-scope endpoints simultaneously as released. There is no phased rollout or pilot group deployment in the standard service offering.

This approach supports several MSSP-grade service objectives:

- Consistent security posture across the customer fleet
- Simplified operational management and reduced complexity
- Faster time to compliance for critical updates
- Clear, predictable behaviour for customers and end users

Customers requiring pilot groups or phased deployment must engage their Account Manager to discuss enhanced service options. These involve additional operational complexity, extended patch cycles, and dedicated resources for pilot monitoring and decision-making.

Application Dependency Awareness

Where known application dependencies exist (such as client-server applications requiring coordinated patch levels), customers must notify Infotrust via their Technical Delivery Manager. Dependencies are documented in the CMDB and may require adjusted deployment sequencing to maintain application functionality.

Infotrust will flag known dependencies identified through Infotrust's Management Platform telemetry and environmental discovery. However, customers retain responsibility for notifying Infotrust of any business-critical application dependencies that may not be visible through standard monitoring. Dependency coordination requires advance notice and should be raised as early as possible, ideally prior to enrolment.

2.8. Rollback Method

Rollback Capability and Limitations

Windows patch rollback is available but carries significant limitations and risks, making it a last resort option rather than a routine practice. Rollback is considered only when a patch causes widespread system instability or failures across multiple customer endpoints, critical business applications are broken by the patch with no workaround available, or in extremely rare cases where security patches create more risk than they mitigate.

The risks of rollback include potential system instability from incomplete removal, security vulnerability exposure if rolling back security patches, and time-consuming manual process for each affected endpoint. These risks must be weighed against the impact of leaving the problematic patch in place.

Rollback Authority

Rollback decisions require appropriate authority based on scope and risk:

Scope	Authority Required	Notification
Single endpoint, non-security patch	Service Desk Engineer	Customer via incident record
Multiple endpoints (<10), non-security patch	Engineering Team Leader Technical Delivery Manager Customer Principal	Customer via incident + phone call

Any security patch rollback	Engineering Team Leader Technical Delivery Manager Technical Operations Manager Customer Principal	Immediate escalation, documented in Risk Register
Fleet-wide rollback (>10 endpoints)	Engineering Team Leader Technical Delivery Manager Technical Operations Manager Customer Principal	Immediate escalation, documented in Risk Register

This authority matrix ensures rollback decisions (particularly those affecting security posture) receive appropriate scrutiny and customer involvement.

2.9. Compliance and Metrics

The following metrics define Infotrust's operational standards for endpoint patching compliance and programme effectiveness. These are internal service objectives, not contractual commitments. SLA commitments are defined in each customer's managed services agreement or statement of work.

Compliance Metrics

The following metrics track endpoint patching compliance and programme effectiveness:

Metric	Target	Measurement Frequency	Reporting
Fleet compliance - **Critical patches**	⩾**92%** of endpoints within 7 business days of patch release	Monthly	Customer monthly report
Fleet compliance - **Standard patches**	⩾**90%** of endpoints within 7 business days of patch release	Monthly	Customer monthly report

Customer Reporting

Monthly compliance reports provide customers with visibility of fleet patch status, including overall compliance percentage, breakdown by patch category, non-compliant endpoints , and trend analysis. Reports reflect the state of the environment as recorded in the management platform at the time of generation.

Configuration of exceptions, exclusions, and remediation planning occurs separately through the customer's Technical Delivery Manager and is not reflected in reporting until changes are enacted in the system.

3. Exception and Risk Acceptance

Customers operating endpoints outside policy requirements must follow the formal exception process. Exceptions are not permanent and require regular review to ensure they remain appropriate as circumstances change. All exceptions are managed through the Managed Services Risk Register to maintain visibility and accountability.

3.1. Exception Requests

Customers submit written exception requests via ServiceNow or through their Technical Delivery Manager (TDM). Each request must identify the system and CMDB reference, specify which policy requirement cannot be met, provide business or technical justification, propose alternative controls or mitigations, and state the requested exception duration.

This structured approach ensures Infotrust has the information necessary to conduct meaningful risk assessment and customers have considered alternatives before seeking exceptions.

3.2. Risk Assessment

The assigned Technical Delivery Manager conducts and documents risk assessment for each exception request in consultation with the customer. The assessment examines security vulnerabilities introduced by non-compliance, stability and supportability implications, impact on interconnected systems, support limitations and exclusions, potential business impact, and recommended mitigating controls.

Risk assessments are provided to customers within 5 business days of exception request, allowing timely decision-making while ensuring thorough analysis.

3.3. Risk Register Management

All approved exceptions are recorded in the Managed Services Risk Register. The register maintains a comprehensive view of accepted risks across the customer base and enables portfolio-level risk management.

Each risk register entry includes:

- Customer and system identification
- Policy requirement being excepted
- Risk rating and description
- Approved exception duration
- Review frequency and next review date
- Customer signatory and acceptance date
- Mitigating controls in place

The Technical Delivery Manager is responsible for maintaining current risk register entries for their assigned customers.

Once an exception is approved and added to the Risk Register, the Technical Delivery Manager notifies the operational delivery teams of the exception and any necessary adjustments to service delivery. This ensures operations teams are aware of endpoints operating under exception and can adjust monitoring, alerting, support procedures, or resource allocation as required.

Operational teams update relevant documentation, runbooks, and ServiceNow configurations to reflect the exception status and any special handling requirements.

3.4. Customer Risk Acceptance and Waiver

Exceptions require formal risk acceptance by the customer through a signed waiver. The waiver documents understanding of identified risks, acceptance that Infotrust cannot be held liable for incidents or breaches resulting from endpoints operating outside policy, acknowledgement of support limitations and SLA exclusions where applicable, agreement to exception review cycle, and confirmation of signatory authority to accept risk on behalf of the organisation.

Exceptions are not active until the signed waiver is received and the exception is added to the Risk Register. This ensures customers make informed decisions with appropriate authority and creates clear legal protection for Infotrust when providing services outside standard policy parameters.

3.5. Exception Review Cycle

All exceptions are reviewed regularly through the customer's scheduled service review meetings with their Technical Delivery Manager. Standard exceptions are reviewed during quarterly business reviews as a minimum. High-risk exceptions are reviewed monthly to ensure elevated risks remain acceptable and controlled. End-of-life system exceptions are reviewed at every service review meeting given the rapidly increasing risk as these endpoints age without vendor support.

During reviews, the TDM and customer assess whether the exception is still required, whether the risk profile has changed, whether mitigating controls remain effective, whether any incidents or issues have occurred related to the exception, and whether a path to compliance now exists.

Review outcomes are documented in the Risk Register, and waivers are refreshed annually or when risk profiles change materially.

3.6. Exception Limits

To maintain service delivery standards and security posture, several limits apply to exceptions. No more than 20% of a customer's managed endpoints may operate under exception, ensuring exceptions remain genuine exceptions rather than becoming the norm. Exceptions for end-of-

life endpoints are time-limited to a maximum of 12 months, encouraging replacement or upgrade planning. Exceptions cannot be used to indefinitely avoid necessary upgrades or replacements.

Where exception limits are approached, the Technical Delivery Manager works with customers on remediation roadmaps to bring endpoints back into compliance progressively.

3.7. Exception Closure and Reinstatement

Once endpoints are returned to compliance, the exception lifecycle concludes. The Technical Delivery Manager closes the exception in the Risk Register with documented justification, notifies operational delivery teams that standard service delivery resumes, and confirms with the customer that the exception is no longer required.

The system is re-enrolled in standard preventative maintenance, SLA coverage is reinstated, and the system is included in standard compliance reporting. The closed exception remains in the Risk Register for audit purposes with a "Closed" status and closure date.

4. Responsibilities

4.1. Infotrust Managed Technology

Infotrust is responsible for the operational execution of this policy. This includes maintaining and communicating preventative maintenance standards, executing patching and update activities, providing compliance monitoring and reporting, and notifying customers of required maintenance or policy exceptions.

Infotrust maintains the tooling and automation platforms that enable effective preventative maintenance at scale, conducts risk assessments for exception requests, and documents all maintenance activities in Infotrust's Management Platform. The policy is reviewed and updated regularly to reflect changing technology and threat landscapes.

Infotrust staff are trained on preventative maintenance procedures to ensure consistent, professional delivery of services across the customer base.

4.2. Customers

Customers play a critical role in enabling effective preventative maintenance. Their responsibilities include:

- Communicating blackout periods to Infotrust with a minimum of 30 days notice, and acknowledging that patching compliance targets may be affected during blackout periods.
- Notifying Infotrust of any endpoints operating in a server-like capacity (such as file hosting or application hosting), business-critical application dependencies, or any circumstances that may require adjusted patching behaviour. These should be raised with the customer's Technical Delivery Manager prior to enrolment where possible.
- Communicating Infotrust's patching and reboot policy to end users to ensure awareness of expected device behaviour during and following patch deployment.
- Maintaining valid vendor licensing for all managed endpoints, as unlicensed or expired software may prevent successful patch deployment.
- Completing any required application or business process testing following patching and notifying Infotrust promptly of any issues identified.
- Funding endpoint upgrades or replacements when devices reach end-of-support, recognising that Infotrust cannot maintain endpoints on unsupported operating systems indefinitely.
- Maintaining appropriate insurance and business continuity arrangements, as preventative maintenance reduces but does not eliminate all operational risk.

4.3. Third Party Vendors

Where third-party vendors provide components of managed systems, they must support Infotrust's ability to maintain those systems effectively. Vendors must provide timely security and patch notifications, support Infotrust's access requirements for maintenance activities, and coordinate their maintenance windows with Infotrust activities.

Vendor-initiated changes must follow Infotrust change governance where they affect managed systems, ensuring appropriate coordination and customer communication.