xcitium
The Power of Zero. Unleashed.

SAFE DEPLOYMENT PRACTICES

Xcitium Security Client (XCS) and Comodo Internet Security (CIS)

Version 1.0 | Effective Date: April 23, 2026

Applicable Products	Xcitium Security Client (XCS), Comodo Internet Security (CIS)
Effective Date	April 23, 2026
Document Version	1.0 – Final

1. Overview

This Safe Deployment Practices (SDP) document outlines the structured, risk-aware approach used to ensure secure software deployment.

It provides a high-level overview of Xcitium's deployment practices. The practices described may vary depending on product version, deployment environment, and customer configuration.

2. Rollback & Recovery Mechanism

Rollback Process

The rollback process is manual for both Enterprise and Consumer versions.

Channel	Rollback Approach
Enterprise	Support team monitors deployment health and production metrics. Rollback may be executed per individual enterprise customer where applicable.
Consumer	Monitoring is primarily based on user feedback and support signals.

Recovery Tools

Offline tools are available to support teams for complete removal of XCS or CIS in critical scenarios.

3. Security & Compatibility Testing

Test Scope

- Latest Windows 11 version
- Previous Windows 11 version
- Latest available Windows preview build

Testing Methodology

- Manual testing for new functionalities
- Automated regression testing
- Compatibility validation across OS versions

4. Monitoring & Metrics

Key Metrics Tracked

- Number of new version instances
- Update trend analysis
- Production incidents per version and per customer

Automated Telemetry

Proprietary telemetry solutions help evaluate the overall success of the release and provide real-time deployment insights.

5. Staged Rollout & Communication

Component	Details
Enterprise Beta Group	Selected customers interested in early access to new functionalities.
Consumer Notifications	Users receive update notifications via forums and in-product messaging 4 weeks post-release.
Release Suspension Criteria	If a high number of incidents are observed in early rollout phases, the release may be paused for further evaluation based on internal assessment.

6. Incident Response

Support Availability

L1/L2/L3 teams are generally available 24/7 for critical incidents and can conduct remote troubleshooting on endpoints.

Automated Incident Handling

- Automatic ticket creation mechanisms are in place upon receiving incident notifications.
- Service Desk platform for users to create tickets independently.

7. Conclusion

Xcitium adheres to a robust, iterative deployment strategy, ensuring security, reliability, and performance across all supported platforms. Continuous monitoring, staged rollouts, and defined rollback mechanisms empower both Enterprise and Consumer customers with a safe and reliable security experience.

These practices are continuously reviewed and updated as part of Xcitium's commitment to product reliability and security.

Disclaimer

This document is provided for informational purposes only and does not constitute a binding commitment. Xcitium reserves the right to modify its deployment practices, processes, and timelines at its discretion without prior notice. No warranties or guarantees are provided regarding the completeness or accuracy of this information. Deployments should always be performed in a test environment prior to use on commercial or operational systems.