Safe Deployment Practices (SDP) Document

For Rising Endpoint Security Software & Driver Release

Release Date: 2026

1. Introduction

To guarantee end-user system stability and security, Beijing Rising Network Security Technology Co., Ltd. follows Microsoft Safe Deployment Practices for all releases of endpoint security software, drivers and signature updates. This document describes our release verification workflow, progressive deployment strategy, monitoring mechanism, rollback capability and exception handling process. It covers full-range product releases including security software and kernel-mode drivers, and aligns with Rising internal product release testing system specifications.

2. Tenets of Safe Deployment Practices

2.1 Roll out changes progressively

Rising adopts a multi-stage progressive exposure deployment model for all software, driver and signature updates. Each release must pass sufficient verification at each stage before expanding to broader user groups.

- Internal Testing Phase: All new releases go through comprehensive internal testing, including functional validation, compatibility test covering multiple Windows desktop and server OS versions, long-duration stability stress test, memory-leak detection, digital-signature validation and security vulnerability scan. Defects found in this phase will be fixed before entering pre-production validation.
- Pre-production Verification: Releases are validated in pre-production environments with representative real-world scenarios, to verify stability, resource consumption and compatibility before external roll-out.
- Canary Controlled Release: New versions are first rolled out to a controlled small-scale group, including internal staff and selected test users. Multiple monitoring metrics are closely observed during the observation window. No fixed static user proportion is hard-coded; the actual scope is dynamically adjusted according to release risk level.
- Progressive Expansion: If the canary phase shows stable metrics without critical anomalies, the release scope will be gradually expanded in batches towards full deployment. Observation

periods are reserved between each expansion wave for health assessment. Release expansion may be paused at any time if abnormal signals are detected.

User grouping for phased roll-out adopts multi-dimension strategies, including user attributes, geographic segmentation, and operating-system environment grouping. The exact grouping scope is dynamically adjusted based on release risk assessment.

Key health-monitoring metrics are tracked throughout each deployment wave, including crash rate, performance degradation rate, key-function failure rate and end-user complaint rate. Deployment expansion can be explicitly paused at any stage upon detecting abnormal signals.

2.2 Treat every change to production equally

All production-bound changes, including major version releases, driver updates and minor hotfix adjustments, shall follow the complete release workflow consistently. Before any release goes live, the following artifacts must be completed:

- Complete test report covering function, compatibility, performance and security items
- Digital-signature verification for binaries and driver packages
- Internal release approval checklist sign-off

2.3 Automate validation and rollback

Automated Validation: Automated test suites are executed for every release candidate, covering functional regression, resource-occupancy monitoring, system-crash simulation and signature-compliance verification.

Automatic Rollback Mechanism: When predefined anomaly thresholds are hit during phased deployment, the system will trigger automatic response workflows. Deployment distribution will be stopped, rollback instructions will be pushed to endpoints, and trouble tickets will be automatically submitted to corresponding R&D teams.

Dual-direction Manual Rollback Capability:

- Management-side rollback: Administrators can trigger rollback for partial or all target endpoints via management console.
- Local endpoint rollback: End-agent supports manual rollback to previous stable version, and rollback can be performed independent of network connectivity. Endpoints locally cache historical stable versions to support offline roll-back.

2.4 Integrated False-Positive & Stability Protection

- System-environment compatibility validation covers mainstream desktop and server Windows operating-system variants. Long-running stress tests are executed to verify no blue-screen, crash or deadlock behaviors.
- Driver signature compliance check is enforced for all kernel-mode driver artifacts.
- Resource-occupancy monitoring is performed to control idle-state CPU overhead and detect memory leaks.
- Critical-system-file protection logic is built-in to reduce false-positive risks for operating-system core components.

3. Risk Control and Rollback Strategy

Every released version maintains unique version identifiers, signature records and release timestamps.

Automatic roll-back trigger criteria:

- Sustained elevated crash rate within observation window
- Key-function failure rate exceeds defined threshold
- Significant performance degradation compared against baseline benchmark

Manual roll-back can be initiated by operation-management team through management console or on-demand customer support requests.

End-points keep local cache of multiple historical stable versions to ensure roll-back availability even under offline network conditions. Emergency hot-fix channels are available for responding to severe security incidents.

After any rollback-triggered incident, engineering teams will conduct post-incident review, identify root-causes, and feed improvements back into test cases and release workflows to prevent recurrence of similar issues.

4. Release Approval Process

Before formal release, test deliverables shall be completed by test team with full test data, result analysis and risk assessment. The approval chain follows: Test Report → Product Manager → R&D Director → Security Committee → Quality Committee → Release Execution Team.

- Test Manager confirms zero critical blocking defects;

- Performance engineer verifies performance attenuation stays within acceptable range;
- Security expert confirms high-risk vulnerabilities are eliminated;
- Operation-team validates stability metrics from phased-release monitoring.

Only after full approval across all roles can the release execution team start official distribution.

5. Emergency Hotfix Release Provision

For urgent security-response scenarios, the workflow supports accelerated release procedures. Even under emergency conditions, minimal quality gates, basic monitoring requirements and roll-back capabilities remain mandatory. Risk assessment will be documented for every emergency release.