Huorong Antivirus Implementation Guide for Meeting Section 2 Safe Deployment Practices (SDP) Requirements

Background and Objectives

In the context of evolving Windows systems and dynamic security threats, security product deployment must balance compatibility and reliability to mitigate risks such as system crashes or protection failures caused by improper deployment.

As a cross-version Windows security solution, Huorong Security Software must comply with the core SDP requirements:
① **Publish SDP documentation** detailing a progressive deployment strategy for Windows updates (e.g., limited testing before broad rollout). Monitor deployment via health signals (e.g., system stability metrics, protection module status) and user feedback.
② **Establish automated rollback mechanisms** to swiftly revert to a stable version upon detecting kernel conflicts or functional anomalies during compatibility testing. Validate recovery efficiency through simulated failure scenarios.
③ **Join the Security Update Validation Program (SUVP)** to conduct pre-release testing of Windows security updates and major releases (e.g., RTM), ensuring deployment alignment with OS version iterations.
Ultimate Goal: Standardize deployment processes and risk controls to maintain endpoint stability during synchronized Huorong-Windows updates.

I. SDP Framework Architecture

Huorong's SDP framework adopts a "**Progressive Control – Rapid Recovery**" approach with four layers:

1. **Policy Management Layer**: Develop SDP documentation per product specifications and Microsoft MVI requirements.
2. **Deployment Execution Layer**: Implement phased rollouts and feature flag controls.
3. **Monitoring & Analytics Layer**: Trigger alerts via multi-dimensional health signals and user feedback.
4. **Emergency Response Layer**: Execute automated rollback and failure recovery workflows.

II. Policy Management Layer: Standardized Documentation

1. **Huorong SDP Documentation Publication**
    - **Content Requirements**:
        - *Progressive Deployment*: Define tiers: **Limited Test** (100K users), **Moderate Rollout** (500K users), **Broad Rollout** (2M users), **Full Deployment** (unrestricted).
        - *Health Signal Thresholds*:
            - Functional complaints: **<5 reports**
            - System crash rate: **<0.05%**

        - Module load failure rate: **<0.1%**
    - **Submission**: Upload updated PDF via https://aka.ms/mvi or https://aka.ms/macp.

III. Deployment Execution Layer: Phased Controls

1. **Progressive Rollout**
    - **Canary Testing**:
        - Target limited user groups for early validation.
        - Monitor functional correctness/stability at Limited/Moderate tiers.
        - Proceed to Full Deployment after validating Broad Rollout.
    - **Stage Entry Criteria**: Zero P1+ defects within **24h (Limited Test)**, **48h (Moderate Rollout)**, **72h (Broad Rollout)**, **6d (Full Deployment)**. Else, trigger rollback or hotfix.
2. **Dynamic Feature Control**
    - Suspend deployments via Huorong's rollout system upon P1+ defects to contain compatibility issues.

IV. Monitoring & Analytics Layer: Health Signals

Dimension	Metric	Alert Threshold	Data Source
System Stability	Hourly BSOD incidents	≥0.1 / hour	Customer Feedback Platform
Resource Usage	Peak CPU usage (non-scan state)	>20% sustained for 10m	Customer Feedback Platform
Module Compatibility	Driver loading failure rate	>5 failures	Customer Feedback Platform
User Feedback	Functional complaints (24h)	≥5 reports	Customer Feedback Platform

---

V. Emergency Response Layer: Rollback & Recovery

1. **Rollback Mechanisms**
    - **Online Rollback**: Execute via Huorong's controlled rollout system.
    - **Installer Rollback**: Distribute stable installers through Huorong's official channels.
2. **Response Workflow**
    - **7-Day Response Cycle**:
        - *Investigation (Day 0-2)*: Analyze crash dumps, driver versions, and logs.
        - *Fix (Day 3-5)*: Internal validation of patched code.
        - *Verification (Day 6-7)*: Canary test (≥100K users) and test report submission.
    - **Resolution Paths**:
        - Deploy fixes via online updates using canary testing protocols.

- Notify users to download updated installers; monitor feedback.

This framework ensures Huorong Antivirus complies with Section 2 SDP requirements, delivering reliable and compatible deployments across Windows environments.