ANTI-ABUSE POLCY FOR .ALIBABA

1. Single Abuse Point of Contact (POC)

The Registry Operator maintains a single, publicly accessible Abuse Point of Contact available 24×7×365, published permanently at nic.alibaba. The POC is reachable via abuse_tld@service.aliyun.com and an online abuse submission form. This applies to all domain names registered under the TLD.

Multi-channel intake & automated classification: All abuse complaints are logged in the Registry Business Operation System (BOS), integrated with Alibaba Cloud's NLP-based analysis module and threat intelligence feeds (Alibaba Cloud Security Center + third-party blacklists) to classify abuse types such as malware hosting, phishing, botnet C&C, or trademark infringement.

SLA response times:
- Auto-acknowledgment: ≤15 minutes;
- Manual triage: ≤4 hours;
- Critical threat mitigation: ≤6 hours (serverHold, DNSSEC DS removal, or EPP updateProhibited)

2. Abuse Complaint Handling & Remediation Policies

Evidence verification: Abuse cases are validated through cross-analysis of DNS query logs, EPP transaction history, and DNS zone changes using Alibaba Cloud CloudMonitor, SLS (Simple Log Service), and Kafka event streams.

Registrar collaboration: Notifications are sent via EPP <poll> messages and email, requiring registrar action within the timeframe defined in the Registry-Registrar Agreement (RRA). Registrars failing to respond promptly may be subject to compliance measures, including suspension of new registrations.
Tiered response:
- Level 1: Notification & Warning;
- Level 2: Lock (serverUpdateProhibited / serverTransferProhibited);
- Level 3: Suspension (serverHold);
- Level 4: Record deletion (extreme cases)

Appeals process: Registrants or registrars can submit appeals via mail; an independent compliance officer (different from the original handler) reviews within 5 business days.

3. Orphan Glue Record Removal

Detection: Daily differential analysis between the PolarDB-X primary registry database and DNSSEC signing server zone data to identify orphan glue (host objects without corresponding parent domains).
Procedure:
- Upon receiving written evidence linking glue records to malicious activity, a Kafka event is triggered to BOS and DNS systems for immediate removal;
- If the registrar does not respond and risk is high, the registry proceeds with removal, retaining full audit logs in SLS.

Rollback safeguard: All removals are preceded by cross-registry host dependency checks; erroneous deletions can be restored instantly from PolarDB hot backups and zone snapshots.

4. WHOIS/RDAP Accuracy

As .alibaba is a brand TLD, registrations are limited to internal entities of the Alibaba Group. All registration data is sourced from verified corporate databases and internal HR systems, ensuring accuracy. With no public registrations, the risk of false WHOIS data is effectively eliminated.

On a quarterly basis, domain WHOIS records are cross-checked against the internal organizational structure and contact databases. Any discrepancies identified are promptly corrected.

5. Additional Registry-level Security Controls

Access & authentication:
- EPP access restricted to whitelisted IPs; TLS 1.2+ with mutual certificate authentication;
- Registrar portal and sensitive EPP operations require MFA (SMS + token);

Change notifications & audit: Domain creation, transfer, deletion, and DS/NS changes are broadcast in real-time to multiple registrar contacts via Kafka; daily summary reports are generated.
Traffic & behavior analysis: Alibaba Cloud Security Center and a proprietary EPP behavioral analysis engine detect and throttle abnormal request patterns (e.g., bulk updates in short time windows).

6. Malicious/Abusive Behavior Definitions & Resolution Metrics

Covered abuse categories: Malware hosting, phishing, botnet C&C, DNS hijacking, fast-flux hosting, CSAM, trademark infringement (URS/UDRP), and other acts requiring takedown by courts or LEA.

KPIs & SLRs:
- MTTA (Mean Time to Acknowledge);
- MTTC (Mean Time to Contain);
- Registrar response rate & remediation compliance rate;
- Orphan glue removal time;
- Recidivism rate monitoring.

Rapid response: High-severity cases resolved within ≤6 hours with serverHold or DNS suspension, synchronized instantly to all DNS nodes (including DNSSEC-signed zones) via BOS + Kafka.

7. Resourcing Plan

The Registry Operator's abuse prevention program is staffed by a dedicated abuse & security engineering team within the registry operations group, supported by Alibaba Cloud's central security, compliance, and legal departments. This allows flexible allocation from a 50+ person registry engineering team to address peak abuse workloads, ensuring continuous 24×7 coverage.

For more information please visit http://nic.alibaba/pdf/AntiAbuse_Policy.pdf