Virtual Earth Nation - Appendix B: Adversarial Participation & Resilience Games (v1.0-textfix)

B.1 Public Program Overview (Friendly Language)

Program Name: Open Security Research & Resilience Games

Purpose: Invite qualified researchers and operators to safely test and improve VEN. We focus on learning, transparency, and user protection.

B.1.1 Eligibility & Onboarding

• KYC/KYB with privacy-preserving options; sign Code of Conduct.
• Complete training: safety, disclosure, synthetic data handling.
• Accept scope-of-work and Rules of Engagement (ROE).

B.1.2 Scopes & Arenas

• Testnets and shadow environments with synthetic data.
• Adversarial Markets with capped value or play-VC.
• Blue/Red Exercises against cordoned subsystems.
• Capture-the-Flag (CTF) and tabletop scenarios.

B.1.3 Rules of Engagement (ROE)

• Written authorization and explicit scope per test.
• No user harm; no real PII; safe payloads only.
• Evidence required: PoC, logs, reproducible steps.
• Coordinated disclosure timelines; fix-first policy.
• Immediate stop and report on accidental spillover.

B.1.4 Rewards & Recognition

• Bug/Exploit bounties (severity and blast radius tiers).
• Resilience points for chaos drills that improve SLOs/MTTR.
• Fraud-prevention prizes measured by prevented-loss uplift.
• Reputation badges and leaderboard standing.
• **Payouts:** WT -> VEX -> VC (optional off-ramp).

B.1.5 Safety & Privacy

• Synthetic or minimized data; capped-value arenas.
• Kill switches and instant rollback.
• Third-party audits of program processes.

B.1.6 Disclosure & Patch

• Severity-based SLAs; emergency hotfix paths.
• Public advisories after fix; researchers credited (opt-in).

B.1.7 Transparency

• Publish quarterly metrics: vulns closed, MTTR deltas, chaos coverage, fraud-prevention uplift.
• Annual public report reviewed by independent oversight.

B.2 Internal Addendum (Restricted Use)

Distribution: SOC/Trust & Safety/Engineering leadership; Oversight Board.

B.2.1 Guild Types (Licensed)

• Red Team Guild: scoped offensive testing, model/red-team prompts, model jailbreak containment.
• Fraud & Market Stress Guild: collusion, wash-trade, payout-abuse simulations.
• Chaos Engineering Guild: fault injection, dependency outages, rollback validation.
• Social Resilience Guild: misinformation/brigading labs, content abuse drills (opt-in cohorts only).

B.2.2 Arena Types & Configuration

• Testnets/Shadow: mirror prod, synthetic users, bounded financial value.
• Adversarial Markets: play-VC or capped-VC, reversible ledgers, supervised oracles.
• Blue/Red Live Drills: cordoned subsystems, maintenance windows, full rollback plans.
• Tabletop/CTF: no prod systems, replayable traces, graded scoring.

B.2.3 Rules of Engagement (Detailed)

Allowed:
• Scoped exploitation, fuzzing, chaos faults, traffic replay with consent.
Prohibited:
• Data exfiltration of real PII, ransom/extortion, irreversible damage, persistence beyond scope, social engineering of non-consenting users.
Evidence:
• Packet/session logs, before/after metrics, PoC artifacts, timeline with UTC stamps.
Disclosure:
• Triage within 24h; severity-based patch windows (Critical: <=72h, High: <=7d, Medium: <=30d, Low: backlog).
Release:
• Publish after fix or after max window with mitigation.

B.2.4 Staking, Slashing, and Bonds

• Entry bond required for high-impact arenas; size scales with potential blast radius.
• Slashing for ROE violations; partial refunds for good-faith errors.
• Repeat-offender lockouts with appeal to Oversight Board.

B.2.5 Safety & Ops Controls

• Change windows; kill switches; golden rollback tests before drill.
• Air-gapped secrets; least-privilege ephemeral creds; session recording for high-privilege actions.
• Dual-approval for production-adjacent drills; independent safety officer sign-off.

B.2.6 Incentives and Tiers

• Severity payouts benchmarked to historic impact and time-to-detect improvements.
• Bonus multipliers for reproducible PoCs and cross-team runbooks.
• Reputation tiers unlock broader scopes and higher payouts.

B.2.7 KPIs & Targets

• Security: MTTD/MTTR reduction vs. baseline; vulnerabilities closed within SLA.
• Fraud: % prevented pre-payout; false-positive rate of detectors.
• Resilience: chaos coverage %, rollback success rate, dependency recovery times.
• Safety: 0 user-harm incidents; compliance audit pass rate.
• Program ROI: payout per critical fix; cost per hour of avoided downtime.

B.2.8 Governance & Oversight

• Ethics & Safety Board: approves scopes, reviews incidents, publishes annual report.
• Immutable audit trail: signed scopes, artifacts, and outcomes.
• Appeals: structured process, time-bounded decisions, remedies.

B.2.9 Legal & Compliance

• AML/CFT at on/off-ramps; export controls; platform-specific policies.
• Child safety: dedicated flows, vetted reviewers, strict retention controls.
• Jurisdiction-aware sanctions and privacy obligations.

B.2.10 Incident Classes

• Sev-0: active exploitation or safety risk -> immediate kill switch, public status page.
• Sev-1: critical vuln without active exploitation -> hotfix within 72h.
• Sev-2+: tracked via backlog with scheduled remediation.

B.3 Interoperability

• Section 2: payouts via WT -> VEX -> VC; anti-hoarding applies.

- Section 3: due process and appeals; sanctions schedules.
- Sections 4-7: drills for infra, services, mobility; Appendix A for airspace and corridors.
- Section 8: credential tiers and access controls for guilds.
- Section 9: SOC, abuse ops, DR/BCP, emergency coordination.

B.4 Roadmap

- Q1: Launch public program and bounty portal; seed CTFs; train first guild cohort.
- Q2: Blue/Red live drills on cordoned systems; publish first resilience report.
- Q3: Expand adversarial markets; add fraud stress league; refine staking tables.
- Q4: Independent external audit; adjust payouts and ROE; scale to partner ecosystems.