

SOP-SEC-2025 — Security & Phishing Protocol

Purpose: Protect Guardian Override systems and contributors from phishing, credential theft, and security breaches. **Scope:** Applies to moderators, Conduct Officers, and technical teams.

Workflow:

1. **Detection:**
 - Automated scans + moderator reports for suspicious links, credential requests, exploit code.
2. **Immediate Action:**
 - Restrict contributor account within 24h.
 - Escalate to Conduct Officers.
 - Notify governance if systemic risk detected.
3. **Classification:**
 - Minor: accidental insecure link → advisory.
 - Moderate: repeated insecure practices → restriction.
 - Critical: phishing, exploit code, credential theft → suspension + law enforcement referral.
4. **Documentation:**
 - Case logged in MEI Appendix E.1.
 - Evidence stored encrypted.
5. **Audit:**
 - Annual penetration testing.
 - Quarterly security incident reports.