Acceptable Use Policy

Rules for Responsible Use of Wardright Public Digital Resources

Effective Date	December 25, 2025
Last Revised	October 14, 2026
Website	https://wardright.com
Legal Contact	contact@wardright.com
Business Contact	405-283-6008 | Mead, Oklahoma, United States

This Acceptable Use Policy (“AUP”) governs use of Wardright LLC public websites, Reference Systems (including Atlas, Relay, and Forge), demonstration workspaces, APIs, forms, upload interfaces, and other public-facing technical resources. It supplements the Terms of Use.

Important: This policy governs Wardright LLC public web properties and business-facing services only. Federal solicitations, awards, subcontracts, NDAs, statements of work, and other executed agreements control where their terms conflict with this public policy.

Contents

Scope • Unlawful Use • Unauthorized Access • Malware • Disruption • Automated Access • Fraud and Impersonation • Harassment and Exploitation • Regulated Misuse • Intellectual Property • Privacy and Data • Credentials • Restricted Government Information • Evasion • Reporting • Enforcement • Changes • Contact

1. Scope and Responsibility

This AUP applies whenever you access or use a Wardright public digital resource or use a Wardright resource as part of a workflow involving third-party systems. You are responsible for your conduct, content, credentials, configurations, automation, and use of outputs.

2. Unlawful or Rights-Violating Use

You may not use Wardright resources to commit, facilitate, promote, instruct, or conceal unlawful activity; infringe or misappropriate copyright, trademark, trade secret, privacy, publicity, contractual, or other rights; unlawfully obtain or disclose personal or confidential information; or evade lawful restrictions, sanctions, court orders, or regulatory obligations.

3. Security Abuse and Unauthorized Access

You may not probe, scan, exploit, or test vulnerabilities of Wardright systems, Cloudflare configurations, networks, accounts, or infrastructure without explicit written authorization. You may not bypass authentication, defeat rate limits or access controls, intercept traffic without authorization, introduce backdoors, or interfere with security logging.

4. Malware and Harmful Code

You may not use Wardright resources to create, deliver, host, distribute, or facilitate malware, ransomware, destructive payloads, credential stealers, botnets, malicious scripts, exploit kits, or code intended to damage, disrupt, surveil, or gain unauthorized control of systems.

5. Service Disruption and Resource Abuse

You may not intentionally degrade, overload, flood, deny service to, disrupt, or materially impair Wardright resources or related infrastructure, or manipulate traffic and requests to bypass protective controls.

6. Automated Access, Scraping, Bots, and Crawlers

You may not use robots, spiders, scrapers, headless clients, automated request systems, or similar means in a manner that defeats technical directives, bypasses access restrictions, degrades service, or collects restricted information without authorization. Ordinary search-engine indexing allowed by technical controls is permitted.

7. Fraud, Deception, and Impersonation

You may not use Wardright resources for phishing, credential theft, fraudulent transactions, deceptive schemes, false procurement communications, impersonation of Wardright, impersonation of a government official or agency, or misrepresentation of sponsorship, endorsement, award status, or government affiliation.

8. Harassment, Threats, and Exploitation

You may not use Wardright resources to facilitate credible threats, stalking, targeted harassment, doxxing, extortion, trafficking, exploitation, or unlawful abuse.

9. Dangerous and Highly Regulated Misuse

You may not use Wardright resources to facilitate unlawful acquisition, manufacture, trafficking, or deployment of weapons, explosives, controlled substances, or other regulated goods, or to provide operational assistance for violent criminal activity. Lawful professional, compliance, engineering, safety, and public-sector activities remain subject to applicable law and contract requirements.

10. Intellectual Property Abuse

You may not remove or falsify copyright, trademark, attribution, licensing, watermark, provenance, or rights-management information in order to misrepresent ownership or facilitate infringement.

11. Privacy and Personal Data

You may not unlawfully collect, infer, expose, trade, or misuse personal information; circumvent privacy settings; obtain credentials; or create databases of sensitive personal information without lawful authority and appropriate safeguards.

12. Credential and Access-Key Abuse

You may not use credentials, API keys, access tokens, accounts, certificates, licenses, or payment methods without authorization. Do not submit credentials or secret material to public Wardright resources.

13. Restricted Government and Customer Information

Public Demonstration Uploads

Forge and any other public upload-enabled Reference System are demonstration environments. Submit only synthetic, non-sensitive files appropriate to the stated demonstration. Do not use them as storage, malware-analysis sandboxes, production document processors, security-testing targets, or transfer mechanisms for confidential, personal, proprietary, controlled, classified, export-controlled, procurement-sensitive, credential, or regulated information. Wardright may reject, quarantine, limit, or delete submissions and generated artifacts for security, capacity, policy, or maintenance reasons.

Unless Wardright has expressly authorized a suitable channel and the governing agreement allows it, you may not submit classified information, CUI, source-selection information, procurement-sensitive information, export-controlled technical data, customer secrets, security keys, or other restricted government or customer information through public website forms, ordinary email, or unauthorised systems.

14. Attempts to Evade Enforcement

You may not evade account restrictions, IP blocks, security challenges, rate limits, access controls, abuse-detection systems, or other enforcement measures through alternate accounts, proxies, credential rotation, spoofing, automation, or similar techniques.

15. Reporting Security Issues and Abuse

If you identify a vulnerability or suspected abuse involving Wardright infrastructure, contact contact@wardright.com with enough information for us to investigate. Do not publicly expose sensitive details, access data that is not yours, or continue testing beyond what is necessary to demonstrate the issue without authorization.

16. Enforcement

Wardright may investigate suspected violations and may warn, rate-limit, block, suspend, restrict, terminate, preserve relevant records, cooperate with providers or lawful authorities, and pursue legal remedies where appropriate.

17. Changes to This AUP

We may update this AUP as threats, services, infrastructure, contracts, or legal requirements evolve.

18. Contact

Legal, security, or abuse reports: contact@wardright.com.

Business telephone: 405-283-6008.

Website: https://wardright.com.