DeployReady Acceptable Use Policy

Effective Date: April 22, 2026
Version: v1.0.0
Last Updated: April 22, 2026
Published at: capstonehorizon.com/legal/aup
Contact: security@capstonehorizon.com

1. Intent

DeployReady is a platform for analyzing federal solicitations and generating proposal drafts. It is designed for businesses pursuing government contracts using publicly available information. This Acceptable Use Policy ("AUP") defines what you may and may not do with the Service. It applies to all customers, users, and anyone accessing the platform. Violations of this AUP may result in suspension or termination under our Terms of Service.

This AUP supplements the Terms of Service. Capitalized terms not defined here have the meanings given in the Terms of Service.

2. Prohibited Uses

You may NOT use DeployReady for any of the following:

2.1 Uploading Prohibited Data.
You may not upload, transmit, or store Prohibited Data as defined in Terms of Service Section 4. This includes Federal Contract Information (FCI), Controlled Unclassified Information (CUI), Classified National Security Information, ITAR-controlled technical data, EAR export-controlled data, Protected Health Information (PHI), and any information protected under DFARS 252.204-7012 or equivalent flow-down clause. DeployReady is not designed or authorized to handle restricted government information.

2.2 Classified or Sensitive Government Work.
You may not use the Service for any proposal work involving classified programs, Special Access Programs (SAPs), ITAR-restricted solicitations, or any procurement where the underlying solicitation is not approved for public release. If a solicitation requires a DD Form 2345 (Militarily Critical Technical Data) or similar access control to download, do not upload it to DeployReady.

2.3 Reverse Engineering or Competitive Intelligence Against Capstone.
You may not use the Service to study, probe, or reverse engineer the DeployReady platform in order to build a competing product, identify proprietary algorithms, or replicate the proposal engine's functionality. You may not use generated outputs to train a competing AI system.

2.4 Systematic Data Collection.
You may not use automated tools, bots, or scripts to extract, collect, or aggregate data from the Service beyond what the authorized API or user interface provides for normal use.

2.5 Submission of False Company Profile Information.
You may not enter false, fabricated, or materially misleading information in your company profile. Your profile is the authoritative source for proposal generation. Submitting false information (false past performance

citations, non-existent personnel, clearances you do not hold) violates this AUP and may constitute fraud under 18 U.S.C. § 1001 if the resulting proposal is submitted to the government.

2.6 Circumventing Tenant Isolation.
You may not attempt to access, read, or modify data belonging to another tenant. You may not probe the application for tenant-isolation vulnerabilities, attempt session hijacking, or attempt to manipulate the `tenant_id` binding in any request.

2.7 Malware and Destructive Uploads.
You may not upload files that contain malware, ransomware, trojans, or other malicious code. You may not use the Service in any attempt to attack or degrade Capstone's infrastructure or that of its subprocessors.

2.8 Spam and Abuse.
You may not use the Service to send unsolicited commercial communications. You may not use your account to relay spam through any Capstone-controlled system.

2.9 Illegal Activity.
You may not use the Service for any purpose that violates applicable law, including export control laws, anti-bribery laws (FCPA, UK Bribery Act), procurement integrity laws (41 U.S.C. § 2101 et seq.), or any other applicable federal, state, or local regulation.

2.10 Harassment.
You may not use the Service to harass, threaten, or intimidate any individual, including Capstone personnel.

3. Fair Use and Resource Limits

3.1 Reasonable Use. DeployReady is a multi-tenant service. You agree to use the Service in a manner that does not disproportionately burden the platform's shared infrastructure. Reasonable use means using the platform for its intended purpose (solicitation analysis and proposal generation) at volumes consistent with normal business activity.

3.2 Rate Limits. Capstone may apply rate limits on API calls, proposal generation requests, and file uploads. Current limits are published in the application. Capstone may adjust rate limits with notice.

3.3 Storage. Each tenant is allocated a reasonable file vault storage capacity as specified in the plan description. Capstone may notify you if your usage approaches plan limits and work with you on a solution.

4. Enforcement

Capstone enforces this AUP progressively, proportionate to the severity and frequency of the violation:

Stage	Trigger	Action
Warning	First minor violation (e.g., excessive rate of requests, minor policy deviation)	Written notice by email
Suspension	Repeated minor violations, or a single significant violation (e.g., circumvention attempt, false profile data)	Temporary account suspension pending investigation

Stage	Trigger	Action
Termination	Severe violation (e.g., Prohibited Data upload, malware upload, circumvention of tenant isolation)	Immediate account termination; Section 4 indemnification applies

For Prohibited Data violations (Section 2.1), Capstone may suspend immediately without a prior warning, consistent with Terms of Service Section 4.5.

Capstone reserves the right to preserve and disclose account information, logs, and content to law enforcement if required by law or if Capstone reasonably believes that disclosure is necessary to protect the rights, property, or safety of Capstone, its customers, or others.

5. Reporting Abuse

If you observe a violation of this AUP, including suspected unauthorized access, malicious uploads, or Prohibited Data in the system, report it to:

security@capstonehorizon.com

Include a description of what you observed, any relevant URLs or account identifiers, and your contact information. All reports are treated as confidential to the extent permitted by law.

For vulnerability disclosures or suspected security issues with the platform, use the same address. Capstone commits to acknowledging vulnerability reports within 2 business days and providing a remediation timeline within 10 business days.

Contact

Capstone Horizon LLC
7782 Rose Rock Way, Las Vegas, NV 89113
security@capstonehorizon.com
capstonehorizon.com