Vulnerability Disclosure Policy

PURPOSE

This Vulnerability Disclosure Policy establishes a process for individuals to responsibly report potential security vulnerabilities in systems owned or operated by Acosta Inc. and its subsidiaries (collectively referred to as the “Company” or “Acosta Group”). It also outlines the Company’s expectations for such reporting and its commitment to appropriately review, investigate, and remediate reported issues.

INTRODUCTION

We are committed to maintaining the security and privacy of our systems, data, and users. We value the contributions of the security research community and welcome responsible disclosure of vulnerabilities that may impact the confidentiality, integrity, or availability of our services.

This Vulnerability Disclosure Policy outlines how to report potential security issues and what you can expect from us in return.

SCOPE

This policy applies to:

- Public facing websites and applications owned or operated by the Company
- Public APIs and associated services
- Cloud hosted infrastructure and assets under our direct control

The following are out of scope unless explicitly authorized:

- Social engineering (phishing, vishing, impersonation)
- Physical security testing
- Denial-of-Service (DoS) or stress testing
- Use of automated scanners that may impact system stability
- Third-party platforms or services not owned by us

If you are unsure whether a system is in scope, please contact us before testing.

REPORTING A VULNERABILITY

If you believe you have discovered a security vulnerability, please report it to us promptly using the following process:

HOW TO REPORT

Send an email to: AskCompliance@acosta.com and include the following details:

- Description of the vulnerability
- Steps to reproduce the issue
- Impact assessment (if known)
- Any supporting evidence (screenshots, logs, proof-of-concept)
- Your contact information for follow-up

We encourage encrypted communication. Our PGP key is available on request.

OUR COMMITMENT TO YOU

When you report a vulnerability in good faith and follow this policy, we commit to:

- Acknowledging receipt of your report within 5 business days
- Providing regular updates on remediation progress
- Working with you to validate the issue
- Not pursuing legal action for good-faith research conducted within this policy
- Crediting you publicly (optionally) once the issue is resolved

RESEARCHER EXPECTATIONS

We ask you:

- Act in good faith and avoid privacy violations
- Do not access, modify, or delete data
- Do not disrupt services or degrade performance
- Give us a reasonable amount of time to remediate before public disclosure
- Comply with all applicable laws

SAFE HARBOR

We support safe-harbor principles for security research. If you adhere to this policy:

- We consider your research authorized
- We will not initiate legal action
- We will work with you to resolve any unintentional impact

This safe harbor does not apply to actions that are malicious, exploitative, or intentionally harmful.

RECOGNITION

We appreciate the efforts of security researchers who help us improve our security posture. With your permission, we may publicly acknowledge your contribution to our Security Hall of Fame page.

POLICY UPDATES

We may update this Vulnerability Disclosure Policy at any time. The latest version will always be available on our website.