JustPark

Vulnerability Disclosure Policy

Vulnerability Disclosure Policy Details	
Last Updated	12/18/2025
Document Version	1.1
Document Owner	Matt Tschoegl
Minimum Review Frequency	Annually
Last Reviewed	12/18/2025
Compliance	CIS Control
Revision history is tracked at the end of the document	

Table of Contents

Overview

JustPark follows the guidance and recommendations provided by the Center for Internet Security (CIS) within the Critical Security Controls documentation and from the Cybersecurity & Infrastructure Security Agency (CISA). This policy aligns primarily with **CIS Control 17** (Incident Response Management) and is supported by **CIS Control 7** (Vulnerability Management), which outlines best practices for discovering, prioritizing, and remediating known vulnerabilities. The policy emphasizes the detection and handling of vulnerabilities through external disclosures and responsible researcher engagement.

Purpose

This policy establishes a standardized approach for external security researchers and members of the public to responsibly report security vulnerabilities. It defines JustPark's commitments, safe harbor provisions, and the process for receiving and responding to vulnerability disclosures, including provisions for discretionary rewards considerations.

Scope

This policy applies to all JustPark-owned and operated systems, including websites, applications, APIs, mobile apps, and infrastructure. Any vulnerabilities with third-party systems not owned or operated by JustPark should be reported directly to the respective vendors.

The policy applies to all external researchers, users, partners, and any individual submitting an unsolicited vulnerability report.

Control Summary

JustPark leverages the list of applicable Safeguards for **CIS Control 17**, for best practice guidance:

Safeguard #	Safeguard Descriptions
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents
17.4	Establish and Maintain an Incident Response Process
17.9	Establish and Maintain Security Incident Thresholds

Policy

JustPark welcomes and values contributions from the security community. JustPark **will not pursue legal action** against researchers, named or anonymous, who act in good faith and follow this policy.

To ensure a safe and constructive process, please adhere to the following:

- Do **not** exploit any vulnerability beyond what is necessary to demonstrate the issue.
- Do **not** access, alter, or delete data that does not belong to you beyond minimal demonstration.
- Do **not** engage in actions that could disrupt services (e.g., denial-of-service attacks).
- Do **not** use phishing, social engineering, or physical intrusion tactics.
- Do **not** perform automated scanning without prior permission.

If you're unsure whether your actions fall within acceptable limits, please **reach out before proceeding**.

We support **Coordinated Vulnerability Disclosure (CVD)**. Public disclosure is permitted **only after** the vulnerability has been addressed or a fix has been scheduled. Please coordinate timing and details with our security team. Researchers may also request public recognition with their consent.

While JustPark does not currently run a public bug bounty program, we may offer **discretionary rewards** for valid and impactful vulnerabilities. Eligibility and reward amounts are determined based on severity, exploitability, and business risk.

JustPark is unable to issue payments to individuals or entities located in countries subject to sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) or the UK Office of Financial Sanctions Implementation (OFSI).

Procedures

We ask that researchers submit all reports to security@justpark.com. Those reports should include the following:

- A clear description of the vulnerability
- Steps to reproduce (screenshots, logs, etc.)
- Impact assessment
- Any suggestions for remediation (optional)
- Preference to remain anonymous or be publicly credited
- Expressed interest in any discretionary rewards

Once a report is received, we will:

- Acknowledge receipt within 3 business days
- Triage and validate the report
- Provide regular status updates
- Coordinate remediation and disclose responsibly
- Credit the researcher upon request, unless anonymity is preferred
- Distribute rewards, if applicable

Document Handling

This document will be reviewed, approved, and distributed in accordance with the Policy Management process and procedure as defined by JustPark. This policy may also be updated as needed to reflect: changes in the threat landscape; updates to applicable legal or regulatory standards; lessons learned from vulnerability reports and incident response; adjustments to bug bounty operations. All subsequent changes will be logged under the “Revision History” section of this document. This document must be reviewed and updated once per year, at a minimum. Any significant changes that affect this document must be **communicated and updated within 30 days of that change.**

Violations & Penalties

Violations of this policy must be immediately reported to any involved managers and the IT Department. Violating the policy or any of its tenets could result in disciplinary action by the Company depending upon the type and severity of the violation, whether it causes any liability or loss to the Company, and/or the presence of any repeated violation(s).

Revision History

Version	Date of Change	Modified By	Summary of Change
1.0	**08/21/2025**	**Matthew Tschoegl**	**Initial Document**
1.1	**12/25/2025**	**Matthew Tschoegl**	**Added language clarifying that JustPark cannot issue discretionary rewards to individuals in OFAC or OFSI sanctioned countries.**

References

1. CIS Controls VERSION 8
    a. https://www.cisecurity.org/controls
2. Common Vulnerability Scoring System (CVSS) defined and managed by FIRST
    a. https://www.first.org/cvss/
    b. https://www.first.org/cvss/user-guide