Appier Vulnerability Disclosure Policy

1. Our Approach

At Appier, we focus our resources on addressing vulnerabilities that pose a real and immediate risk to our users. This policy is designed to streamline the reporting process for meaningful security findings.

2. Response and Remediation

- Acknowledgement: We aim to respond to high-quality, actionable reports within 7 business days.
- Prioritization: Remediation efforts are prioritized based on the severity, exploitability and the potential impact of the issue; timelines are not guaranteed and may vary accordingly.
- Communication: Our team may reach out to request additional information where needed to reproduce or validate the report.
- Note: Reports that lack a manual Proof of Concept (PoC) or fall under the "Ineligible" list (see Section 6) may not receive an individual response.

3. Submission Guidelines

We ask researchers to:

- Send reports to **security@appier.com**.
- Include a clear Proof of Concept (PoC). We cannot process reports that are purely theoretical or based solely on automated scanner results.
- Act in good faith to avoid privacy violations or service disruptions.

4. Data Privacy & Confidentiality

To protect our customers, users and Appier's assets, researchers must adhere to the following rules regarding data access:

- Stop Immediately: If you inadvertently access sensitive data (including but not limited to PII, customer credentials, or confidential business information), please discontinue testing immediately and notify Appier via **security@appier.com**, along with a brief description of the nature and scope of the data accessed**.**
- Prohibited Actions: Researchers must avoid viewing, downloading, modifying, or transferring any data that does not belong to them, except where absolutely necessary to provide a basic Proof of Concept (PoC).

- Data Deletion: Any data unintentionally accessed or stored during the research process must be securely purged from all your storage locations (including local systems, cloud storage, and any third-party platforms) as soon as practicable after the vulnerability report is submitted to Appier. Upon Appier's request, researchers shall provide written confirmation of such deletion, and Appier reserves the right to request reasonable evidence of secure deletion.
- Strict Confidentiality: All information regarding the vulnerability and any accessed data must be kept strictly confidential and may not be shared with any third party.

5. Safe Harbor

Research should be conducted in good faith and must avoid service disruption, protect user privacy, and refrain from social engineering.

We are committed to working collaboratively with security researchers. We will not pursue legal action against researchers who act in good faith, follow these guidelines, and provide us with a reasonable opportunity to investigate and remediate reported issues prior to any public disclosure. Any public disclosure of the vulnerability must be coordinated with and explicitly approved by Appier in writing. For clarity, this safe harbor does not apply to malicious, reckless, or illegal acts beyond the scope of this policy

6. Ineligible Issues (The "No-Response" List)

To minimize noise and focus on critical threats, the following are **not** eligible for a valid report:

A. Non-Exploitable & Automated Findings

- Automated Scans: Raw outputs from tools (e.g., Nessus, Burp, Nmap) without a manual, validated PoC.
- Theoretical Risks: Use of known vulnerable components or SSL/TLS ciphers without a working exploit.
- Data Leaks: Reports relying on previously breached, leaked, or public data.

B. Security Best Practices & Configuration

- Security Headers: Missing or misconfigured CSP, HSTS, X-Frame-Options, or cookie flags (HttpOnly/Secure).
- Email & DNS: Missing or weak SPF, DKIM, DMARC, or DNSSEC records.
- Information Disclosure: Software version disclosure, banner grabbing, stack traces, path disclosure, or private IP addresses.

C. Low-Impact Web Issues

- User Interface: Clickjacking, Self-XSS, Content Spoofing, or Open Redirects.
- Session & Account: Login/Logout CSRF, session duration/concurrency, user enumeration, or brute-force on login/password pages.
- General Web: CSV Injection, HTTP TRACE/OPTIONS methods, or vulnerabilities affecting only outdated browsers.

D. Operational & Physical Attacks

- Disruption: DoS/DDoS, rate limiting, or any attack requiring physical access to devices.
- Social Engineering: Phishing, vishing, or any attack targeting our employees or users.
- Third-Party: Vulnerabilities on products or services not directly managed by Appier

7. Scope

This policy applies to the following Appier products and services:

- **AdCreative.ai**
- **AIRIS**
- **Woopra**
- **AIQUA**
- **AIXON**
- **AIXPERT**
- **BotBonnie**
- **AiDEAL**

Note: Any service or product not explicitly listed above, including third-party hosted services or integrated platforms, is considered Out of Scope.

8. Rewards

Rewards are strictly discretionary and are reserved only for unique, validated findings involving previously undisclosed vulnerabilities that represent a significant risk. These are evaluated on a case-by-case basis and are not a guaranteed entitlement.