SMACKDAB INC. OFFICIAL POLICY

RESPONSIBLE DISCLOSURE POLICY (VDP)

Official legal PDF. This document is generated from the Smackdab website legal source file.

SMACKDAB INC. RESPONSIBLE DISCLOSURE POLICY (VDP)

Effective Date: April 26, 2025 **Last Updated**: November 1, 2025

Version:

2.0

Document Location: https://smackdab.ai/legal/responsible-disclosure-policy

1. INTRODUCTION & COMMITMENT

Smackdab Inc. ("Smackdab," "we," "us," or "our") is committed to ensuring the security of our services and protecting our customers' data. We value the contributions of the security research community in helping us maintain a high standard of security. This Responsible Disclosure Policy (also known as a Vulnerability Disclosure Policy or "VDP") outlines the process for security researchers ("Researchers," "you," "your") to report potential security vulnerabilities identified in Smackdab's systems and services.

We encourage responsible reporting of vulnerabilities. If you believe you have found a security vulnerability in our systems, please notify us according to the guidelines below. We are committed to working with the community to verify and address potential vulnerabilities reported to us.

2. DEFINITIONS

For purposes of this Policy, the following terms shall have the meanings set forth below:

2.1. "Security Vulnerability" means a weakness in a system or its design that could be exploited to cause a breach of security, unauthorized access, data exposure, or disruption of service.

2.2. "Researcher" means an individual or organization that identifies and reports security vulnerabilities in accordance with this Policy.

2.3. "In-Scope Systems" means the systems, services, and applications specified in Section 3.1 that are covered by this Policy.

2.4. "Out-of-Scope Systems" means the systems, services, and activities specified in Section 3.2 that are not covered by this Policy.

2.5. "Responsible Disclosure" means the practice of privately reporting a security vulnerability to the affected organization, allowing them a reasonable time to investigate and remediate the issue before public disclosure.

2.6. "Vulnerability Severity" means the classification of a security vulnerability based on its potential impact and exploitability. We use the Common Vulnerability Scoring System (CVSS v3.1) to determine severity levels as follows:

- **Critical Severity:** CVSS score 9.0-10.0
- **High Severity:** CVSS score 7.0-8.9
- **Medium Severity:** CVSS score 4.0-6.9
- **Low Severity:** CVSS score 0.1-3.9

---

3. SCOPE

###

3.1. In-Scope Systems

This Policy applies to security vulnerabilities found within the following Smackdab systems and services ("In-Scope Systems"):

- **Primary Website:** https://smackdab.ai and its subdomains
- **Smackdab Application Platform:** https://app.smackdab.ai and related application endpoints
- **Public APIs:** https://docs.smackdab.ai and documented API endpoints
- **Mobile Applications:** Official Smackdab mobile applications for iOS and Android

###

3.2. Out-of-Scope Systems

The following systems, services, and activities are explicitly **OUT OF SCOPE** for this Policy:

- Systems, websites, or services hosted by third-party providers (e.g., partners, integrated services, underlying infrastructure providers like AWS/GCP) unless the vulnerability is directly in Smackdab's configuration thereof. Please report vulnerabilities in third-party services directly to that third party.
- Social media channels operated by Smackdab.
- Physical security of Smackdab facilities.
- Social engineering (e.g., phishing, vishing) of Smackdab employees, contractors, or customers.

- Denial of Service (DoS or DDoS) attacks or activities that could degrade, interrupt, or harm Smackdab services or users.
- Testing that involves accessing, modifying, or destroying data belonging to other Smackdab customers or users.
- Posting, transmitting, uploading, linking to, sending, or storing any malicious software.
- Any activity that violates applicable laws or regulations or disrupts our services.

Discovery of vulnerabilities in out-of-scope systems should not be reported under this Policy. If you are unsure whether a system or vulnerability is in scope, please contact us first at security@smackdab.ai.

###

3.3. Testing Authorization

Before beginning security testing against any authenticated areas of Smackdab's systems, you must:

1. 1. Create a legitimate account for testing purposes
1. Only test against your own account
1. Clearly label test accounts with "SECURITY*TEST*\" as a prefix in any customizable fields

No prior explicit authorization is required for security testing against publicly accessible (unauthenticated) portions of our In-Scope Systems, provided you follow all other guidelines in this Policy.

For high-impact testing (such as testing that might affect system availability or integrity), please contact us at security@smackdab.ai to coordinate your testing activities before proceeding.

---

4. GUIDELINES & RULES OF ENGAGEMENT

We require that Researchers adhere to the following guidelines when investigating and reporting vulnerabilities:

###

4.1. General Guidelines

- **AUP Alignment.** Security research conducted in compliance with this Policy is **not** a violation of the Smackdab Acceptable Use Policy (AUP). Researchers must follow this Policy’s scope and rules of engagement.
- **Personal Data Incidents.** Where a reported vulnerability or incident involves **Personal Data**, notifications to Customers and regulators will follow the timeframes and processes set forth in Smackdab’s **DPA** (processor notice within **48 hours**) and related privacy policies.

- **Act Responsibly:** Conduct your research ethically and in a manner that avoids harm to Smackdab, our customers, our employees, or any third parties.
- **Avoid Privacy Violations:** Do not access, download, modify, destroy, or exfiltrate any data that does not belong to you, especially customer data or personal information. Stop testing and report immediately if you encounter any user data during testing.
- **Avoid Service Disruption:** Do not engage in any activity that could degrade or disrupt our services (e.g., DoS/DDoS attacks, high-intensity automated scanning that impacts performance). Rate limiting may be in effect.
- **Use Authorized Channels:** Report vulnerabilities only through the designated channel specified in Section 5. Do not disclose vulnerabilities publicly or to third parties before coordinating with Smackdab (see Section 8).
- **Scope Adherence:** Only test systems explicitly listed as In-Scope Systems.
- **Good Faith:** Perform research and reporting in good faith. Do not attempt to extort Smackdab or demand compensation beyond any official bug bounty program we may offer.

###

4.2. Permitted Testing Tools and Methods

The following security testing tools and methods are permitted when used responsibly:

- **Manual Testing:** Browser-based testing, API endpoint testing, and manual code review
- **Lightweight Scanning:** Non-invasive vulnerability scanning with tools like Burp Suite, OWASP ZAP, or Nmap when used with reasonable rate limiting (maximum 10 requests per second)
- **Static Analysis:** Analysis of publicly available source code or downloadable applications
- **Client-Side Testing:** Examination of client-side code and application behavior

All automated scanning tools must include your contact information in the User-Agent string or headers (in the format "SecurityResearch-\\\[YourEmail\\\]") to help us identify your legitimate testing activity. Failure to properly identify your testing traffic may result in IP blocking.

###

4.3. Prohibited Activities

Testing against authenticated areas of production systems requires prior written authorization. Unauthenticated, publicly accessible endpoints may be tested without prior authorization provided you comply with §3.3 and all other limits in this Policy.

- Automated vulnerability scanning without rate limiting or coordination

- Testing that impairs or disrupts the availability of systems or services
- Exploitation of vulnerabilities beyond what is necessary to demonstrate their existence
- Disclosure of vulnerabilities to third parties or the public before Smackdab has had reasonable time to address them
- Use of scanners, tools, or techniques that generate significant volumes of traffic or requests

Violation of these guidelines may result in suspension of your access, legal action, or other remedies available to Smackdab under applicable law.

---

5. HOW TO REPORT A VULNERABILITY

If you believe you have discovered a vulnerability within the scope of this Policy, please report it to us promptly by sending an email to:

Email: security@smackdab.ai

Subject Line: "Vulnerability Report: \[Brief Description\]"

###

5.1. Report Content

Please include the following information in your report:

- **Clear Description:** Detailed description of the vulnerability, including the potential impact.
- **Location:** Specific URL, IP address, application area, or API endpoint where the vulnerability was discovered.
- **Steps to Reproduce:** Clear, step-by-step instructions to allow our team to replicate the vulnerability. Include any necessary proof-of-concept code, scripts, screenshots, or network traffic logs (avoid including sensitive data).
- **Supporting Materials:** Any tools, exploits, or technical details that would help us understand and verify the issue. Please remove any sensitive information.
- **Your Contact Information:** Your name and email address for follow-up communications. Anonymous reports may be accepted but limit our ability to follow up or offer recognition.
- **Disclosure Plans:** Any plans you may have for public disclosure (see Section 8).

Please submit one vulnerability per report, unless multiple vulnerabilities are dependent on each other. Use encrypted communication if possible when submitting sensitive details.

###

5.2. Report Template

To ensure a complete report, consider using this structured format:

VULNERABILITY REPORT

Title: \[Brief, descriptive title\]

Date: \[Discovery date\]

Researcher: \[Your name and contact information\]

CVSS Score (if known): \[Score and vector\]

\## Description

\[Detailed explanation of the vulnerability\]

\## Affected System(s)

\[Specific URLs, endpoints, or components affected\]

\## Steps to Reproduce

1. \[First step\]

2. \[Second step\]

3. \[Continue as needed\]

\## Potential Impact

\[Explanation of what an attacker could accomplish by exploiting this vulnerability\]

\## Supporting Evidence

\[Screenshots, logs, or code snippets\]

\## Suggested Mitigation

\[Optional: Your recommendations for addressing the issue\]

\## Disclosure Plans

\[Your timeline or intentions regarding disclosure\]

---

6. OUR COMMITMENTS & PROCESS

Upon receiving a vulnerability report that complies with this Policy, Smackdab commits to:

###

6.1. Acknowledgement

We will acknowledge receipt of your report within **7 business days**. For critical severity vulnerabilities, we aim to provide same-day acknowledgment during business hours.

Our acknowledgment will include:

- A unique reference ID for your report
- Confirmation that the report is within scope
- The name of the security team member assigned to your report
- Estimated timeframe for initial assessment
- Any additional information we may need from you

###

6.2. Triage & Validation

We will investigate and validate the reported vulnerability. This process may take time depending on complexity. We aim to confirm the validity of a report within **30 business days**, though this may vary based on the nature and complexity of the reported issue.

Smackdab reserves the right to reclassify the severity of a vulnerability after our assessment. If we determine a different severity level than what was initially reported, we will provide a clear explanation for the reclassification based on our CVSS scoring methodology.

###

6.3. Vulnerability Management Process

We follow a structured process for managing reported vulnerabilities:

1. **Initial Assessment:** Preliminary review by our security team to determine scope and validity
1. **Classification:** Assignment of severity and priority based on CVSS scoring
1. **Tracking:** Each valid vulnerability is assigned a unique identifier in our internal tracking system
1. **Development Planning:** Remediation tasks are created and assigned to appropriate engineering teams
1. **Remediation:** Implementation of fixes or mitigations
1. **Verification:** Testing to confirm the vulnerability has been properly addressed
1. **Closure:** Final communication with the reporter and internal documentation

For critical vulnerabilities, we may establish a dedicated incident response team to expedite the remediation process.

###

6.4. Communication

We will endeavor to maintain open communication, providing periodic updates on the status of the reported vulnerability as appropriate (e.g., when validated, when remediation is complete). We will notify you when the vulnerability has been validated and again when it has been remediated.

For significant vulnerabilities, we may request a confidential video call to discuss details or clarify certain aspects of the report. In such cases, we may request that you sign a Non-Disclosure Agreement (NDA) before sensitive information is shared.

###

6.5. Remediation

If the report is validated, we will assign resources to remediate the vulnerability in a timeframe appropriate to its severity and complexity. Our target timeframes for remediation are:

- **Critical Severity:** 14 days
- **High Severity:** 30 days
- **Medium Severity:** 90 days
- **Low Severity:** TBD days

These timeframes may be adjusted based on technical complexity, operational constraints, or other factors.

###

6.6. Recognition

We appreciate the effort of security researchers. While Smackdab does not currently offer a formal bug bounty program, we may offer recognition (e.g., acknowledgment on a security researcher list) for valid and responsibly disclosed vulnerabilities at our discretion. Depending on the severity and impact of the vulnerability, we may also offer:

- Public acknowledgment (with your permission)
- Letter of recognition
- Certificate of responsible disclosure
- Swag or other token of appreciation

We evaluate each valid reported vulnerability on a case-by-case basis to determine appropriate recognition.

Eligibility Criteria for Recognition:

- You must be the first person to report a particular vulnerability
- The vulnerability must be previously unknown to Smackdab
- The report must be clear, complete, and follow our reporting guidelines
- You must not have violated this Policy during your research
- You must not publicly disclose the vulnerability before we've addressed it
- You must respond to requests for additional information in a timely manner

###

6.7. Vulnerability Re-testing

After we've notified you that a reported vulnerability has been fixed, you may wish to verify the fix. For re-testing:

- Request permission before re-testing by emailing security@smackdab.ai
- Wait for explicit approval before beginning re-testing
- Limit your testing to only the specific vulnerability you reported
- Follow the same rules of engagement as during initial testing
- Report your findings from re-testing through the same channel

###

6.8. Future Bug Bounty Program

While Smackdab does not currently operate a formal bug bounty program with monetary rewards, we are actively evaluating the implementation of such a program in the future.

---

7. SAFE HARBOR

Smackdab will not initiate or support legal action against Researchers for security research activities that:

- Comply with this Policy;
- Are conducted in good faith and for the purpose of security research only;
- Do not violate applicable law; and

- Do not result in substantial harm to Smackdab, its customers, users, or others.

We consider activities conducted consistent with this Policy to constitute "authorized" conduct under the following laws and regulations:

- Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030
- Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1201
- Electronic Communications Privacy Act (ECPA)
- State computer crime laws similar to the CFAA
- Applicable anti-hacking provisions of state data breach notification laws
- Federal and state laws prohibiting unauthorized access to computer systems
- Federal and state laws prohibiting interception of electronic communications
- Federal and state laws prohibiting circumvention of technological protection measures

If legal action is initiated by a third party against you in connection with activities conducted under this Policy, we will take steps to make it known that your actions were conducted in compliance with this Policy.

This safe harbor applies only to activities focused on the In-Scope Systems and conducted strictly following the Guidelines and Reporting process outlined herein. It does not protect against actions violating laws or this Policy, nor does it apply to out-of-scope systems or activities.

Limitations: The safe harbor provision does not bind law enforcement, regulatory agencies, or other third parties who may take a different view of the activities. While we will advocate for you in such situations (provided you've complied with this Policy), we cannot guarantee protection from enforcement of applicable laws.

---

8. COORDINATED DISCLOSURE & PUBLICATION

###

8.1. Coordinated Disclosure

As a condition of participating in this security research program, you must maintain strict confidentiality regarding any discovered vulnerability until we have confirmed remediation or mutually agreed in writing upon a disclosure timeline. Unauthorized disclosure of vulnerability details may void any safe harbor protections under this Policy.

###

8.2. Standard Publication Timeline

We ask for a minimum of **90 days** of confidentiality after our initial acknowledgement of your report before any public disclosure, to allow for remediation. For complex vulnerabilities, we may request additional time.

###

8.3. Exceptional Timeline Cases

We recognize that standard timelines may not apply to all situations:

- **Critical Vulnerabilities:** For vulnerabilities that pose an imminent and severe risk to users, we may mutually agree to an accelerated timeline.
- **Complex Fixes:** For vulnerabilities requiring significant architectural changes, we may request an extended timeline beyond 90 days. In such cases, we will:
- Provide regular status updates on remediation progress
- Implement temporary mitigations where possible
- Work collaboratively to establish a reasonable disclosure timeline
- **Active Exploitation:** If a vulnerability is being actively exploited in the wild, we will work with you to establish an appropriate timeline that balances user protection and proper remediation.
- **Dependency Issues:** For vulnerabilities in third-party dependencies, timelines may be influenced by the third party's remediation schedule.

We are committed to addressing all vulnerabilities in good faith and as quickly as feasible, and will work with you to establish reasonable timelines for exceptional cases.

###

8.4. Coordinated Publication

If you wish to publish information about a vulnerability after the agreed embargo period:

- Please coordinate with us at least 7 days before publication
- Share your planned publication materials with us for review
- Consider our feedback regarding sensitive details that may still pose security risks
- Include information about the resolution if the vulnerability has been fixed

###

8.5. Ongoing Vulnerabilities

For vulnerabilities that require longer remediation periods, we will work with you to establish a reasonable timeline for disclosure based on:

- The severity and complexity of the vulnerability
- The technical challenges of remediation
- The potential impact on users if disclosed prematurely

---

9. LEGAL CONSIDERATIONS

###

9.1. Compliance with Laws

All security research activities must comply with all applicable local, state, federal, and international laws. Nothing in this Policy is intended to grant permission to violate any applicable laws or regulations.

###

9.2. International Researchers

This Policy applies to researchers globally. However, we acknowledge that laws regarding security research vary by jurisdiction. If you are located outside the United States, please ensure your activities comply with both your local laws and United States laws before engaging in security research activities.

Relevant international cybersecurity and computer crime laws that may apply include:

- **European Union:** Directive 2013/40/EU on attacks against information systems
- **United Kingdom:** Computer Misuse Act 1990 (as amended)
- **Canada:** Criminal Code sections 342.1 and 430(1.1)
- **Australia:** Cybercrime Act 2001 and Criminal Code Act 1995
- **Singapore:** Computer Misuse Act
- **Japan:** Unauthorized Computer Access Law (Law No. 128 of 1999)
- **Brazil:** Law No. 12.737/2012 (Carolina Dieckmann Law)

In jurisdictions where no explicit security research exemptions exist, this Policy may not provide legal protection outside the United States. Researchers should consult local legal counsel if uncertain about legal implications in their jurisdiction.

###

9.3. Limitation of Liability

To the maximum extent permitted by law, Smackdab disclaims any liability for any damages or harm resulting from security research conducted in accordance with this Policy.

###

9.4. Modifications to this Policy

Smackdab reserves the right to modify this Policy at any time. Changes will be published on our website. Security research should be conducted according to the version of the Policy in effect at the time of the research.

---

10. QUESTIONS

If you have questions about this Policy or whether a particular system or activity is in scope, please contact us at security@smackdab.ai **before** starting your research.

---

11. CONTACT INFORMATION

Email: security@smackdab.ai **Mail:** Smackdab Inc. Attn: Security Team 372 Live Oak Ln Marco Island, FL 34145 United States

We also support the security.txt standard (RFC 9116) to help security researchers locate our security policy and contact information. Our security.txt file is available at:

- https://smackdab.ai/.well-known/security.txt
- https://app.smackdab.ai/.well-known/security.txt

This PDF is the formal downloadable version of RESPONSIBLE DISCLOSURE POLICY (VDP).