SMACKDAB INC. OFFICIAL POLICY

TRUST & SECURITY

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

SMACKDAB TRUST & SECURITY

Last Updated: 11/22/2025

At Smackdab, security is not an afterthought—it is a core part of how we design, build, and operate our platform. This page provides a high-level overview of our security practices. For full legal detail, refer to the Smackdab Security Policy and Data Processing Addendum.

- * *

1. SECURITY PROGRAM OVERVIEW

- **Dedicated Security Leadership** – Smackdab maintains a formal information security program led by a designated security leader and supported by a cross-functional security committee.
- **Governance & Risk Management** – We perform regular risk assessments, maintain a risk register, and review major security issues with senior leadership at least quarterly.
- **Policies & Training** – All personnel are subject to written security policies and receive security awareness training during onboarding and annually thereafter.
- * *

2. INFRASTRUCTURE & NETWORK SECURITY

- **Secure Hosting** – Smackdab uses industry-standard data centers with strong physical security and environmental controls.
- **Network Protection** – We employ network segmentation, firewalls, intrusion detection/prevention, and DDoS protections to defend against attacks.
- **Encryption in Transit** – All traffic between customers and the Smackdab platform is protected using TLS (HTTPS).
- * *

3. APPLICATION & DATA SECURITY

- **Secure Development Lifecycle** – Security is integrated into our development process via secure coding standards, code review, static and dynamic analysis, and pre-production security testing.
- **Authentication & Access Control** – We support strong authentication and enforce least-privilege access to production systems, including multi-factor authentication for administrative access.
- **Data Encryption** – Customer data is encrypted in transit and at rest using modern encryption standards.
- * *

4. VULNERABILITY MANAGEMENT & TESTING

- **Automated Scanning** – We perform regular vulnerability scanning of our infrastructure and applications, as well as targeted scans after significant changes.
- **Penetration Testing** – We engage independent third-party security experts for periodic penetration tests of the Smackdab platform.
- **Public Vulnerability Disclosure Program** – Security researchers can report vulnerabilities through our Responsible Disclosure Policy (VDP), which includes safe harbor protections and structured triage.
- **Bug Bounty Program** – Eligible reports may be rewarded under our Bug Bounty Program Terms.
- * *

5. INCIDENT RESPONSE & BREACH NOTIFICATION

- **Formal Incident Response Plan** – Smackdab maintains a documented incident response plan with defined roles, playbooks, and 24/7 monitoring for security events.
- **Rapid Notification** – In the event of a confirmed personal-data breach, we will notify affected customers without undue delay and, in any event, within 48 hours of becoming aware, enabling them to meet their own regulatory obligations.
- * *

6. PRIVACY & DATA PROTECTION

- **Data Processing Addendum (DPA)** – For customers who handle personal data, our DPA describes roles, responsibilities, and data protection commitments under GDPR, CCPA, and similar laws.

- **Application Privacy Notice** – Describes how we process Client Data as a processor/service provider when customers use the Smackdab application.
- **International Transfers** – Where required, we rely on appropriate transfer mechanisms and contractual safeguards.
- * *

---

7. SUB-PROCESSORS

We use carefully vetted Sub-Processors to help deliver our services (for example, infrastructure hosting, email delivery, and support tooling). Each Sub-Processor is bound by contractual security and data protection obligations.

See the **Smackdab Sub-Processor List** for current providers.

- * *

---

8. SECURITY FOR RESEARCHERS

We welcome security research and responsible disclosure.

- **Responsible Disclosure Policy (VDP)** – Defines in-scope systems, rules of engagement, safe harbor, and coordinated disclosure timelines.
- **Bug Bounty Program** – Provides monetary rewards for qualifying reports, subject to the Bug Bounty Program Terms.
- **security.txt** – Our .well-known/security.txt file makes it easy for researchers to find our security contact and policy.
- * *

---

9. QUESTIONS & SECURITY REVIEWS

Customers and prospects who require more detailed information (e.g., security questionnaires, SOC 2 reports, or specific controls mapping) can contact us via:

- Email: **security@smackdab.ai**
- Or through your Smackdab account representative.

For detailed legal terms, please refer to our Security Policy, Data Processing Addendum, and Privacy Policy.

This PDF is the formal downloadable version of TRUST & SECURITY.