SMACKDAB INC. OFFICIAL POLICY

SECURITY POLICY

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

SMACKDAB INC. SECURITY POLICY

Effective Date: April 26, 2025

Last Updated: November 1, 2025

Version:

2.1

Document Location: https://smackdab.ai/legal/security-policy

---

1. INTRODUCTION

This Security Policy ("**Policy**") describes the security practices and measures implemented by Smackdab Inc. ("**Smackdab**," "**we**," "**us**," or "**our**") to protect the security, confidentiality, integrity, and availability of our Services and the data processed through them.

Smackdab is committed to maintaining a comprehensive information security program designed to protect our systems, our Services, and our Customers' data. This Policy outlines the administrative, technical, and physical safeguards we employ to protect against unauthorized access, disclosure, alteration, or destruction of information maintained in our systems.

This Policy is incorporated by reference into the Smackdab Terms of Service and applies to all Smackdab Services. In the event of any conflict between this Policy and the Terms of Service, the Terms of Service shall control unless explicitly stated otherwise. For matters involving Personal Data, the **DPA controls;** for PHI, an executed **BAA** controls; otherwise, the **TOS** controls. Customers, prospective customers, and other interested parties can use this Policy to understand our security practices.

1.1. Security Program Objectives

The primary objectives of our information security program are to:

- Protect the confidentiality, integrity, and availability of Customer Data
- Identify and address security risks in a timely manner
- Prevent unauthorized access to systems and data
- Ensure business continuity and minimize business impact in the event of a disruption

- Comply with legal, regulatory, and contractual requirements
- Promote security awareness throughout our organization
- Continuously improve our security posture in response to evolving threats

1.2. Security Principles

Our security practices are guided by the following principles:

- **Defense in Depth:** Multiple layers of security controls throughout our systems and processes
- **Least Privilege:** Access rights limited to the minimum necessary to perform job functions
- **Separation of Duties:** Critical tasks divided among multiple individuals to prevent fraud or error
- **Data Minimization:** Collection and retention of only necessary data for specified purposes
- **Secure by Design:** Security integrated into the development process from the beginning
- **Zero Trust:** Verification required for all access regardless of source or network location
- **Continuous Improvement:** Regular assessment and enhancement of security controls
- **Risk-Based Approach:** Security resources prioritized based on risk assessment

1.3. Security Policy Framework

This Policy serves as the foundational document in our security policy framework. It is supported by more detailed policies, standards, and procedures that provide specific guidance for different aspects of our security program. Supporting documents include but are not limited to:

- Access Control Policy
- Data Classification and Handling Policy
- Acceptable Use Policy
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan
- Secure Development Policy

These supporting documents are available to Customers upon request, subject to appropriate confidentiality agreements.

2. SCOPE AND APPLICABILITY

2.1. Services Covered

This Policy applies to all Smackdab Services, including:

- The Smackdab SaaS platform and all its modules
- Mobile applications provided by Smackdab
- Smackdab APIs and integrations
- Smackdab-operated websites and portals
- Supporting infrastructure and systems operated by Smackdab
- Smackdab employees and contractors with access to Customer Data

2.2. Data Protection Classifications

Smackdab classifies information into the following categories, with corresponding security controls:

- **Public Information:** Information intended for public disclosure.
- **Internal Information:** Non-sensitive information for internal use.
- **Confidential Information:** Business-sensitive information requiring protection.
- **Customer Data:** All data submitted to the Services by Customers or their Users, which may include personal data or confidential business information.
- **Restricted Data:** Highly sensitive information requiring the strongest protection measures, including certain categories of personal data.

2.3. Security Documentation

This Policy provides a high-level overview of our security practices. Additional detailed security documentation, which may contain sensitive security information, is available to Customers upon request subject to appropriate confidentiality agreements.

3. DEFINITIONS

The following definitions apply to terms used throughout this Policy:

3.1. "Availability" means ensuring timely and reliable access to and use of information and services by authorized individuals.

3.2. "Business Continuity" means the capability of the organization to continue delivery of services at acceptable predefined levels following a disruptive incident.

3.3. "Confidentiality" means preserving authorized restrictions on information access and disclosure, including means for protecting privacy and proprietary information.

3.4. "Customer" means an entity or individual that has entered into an agreement with Smackdab to use the Services.

3.5. "Customer Data" means all electronic data or information submitted by Customer or its Authorized Users to the Services as part of Customer's use of the Services.

3.6. "Data Breach" means a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. Not all security incidents constitute data breaches.

3.7. "Disaster Recovery" means the process, policies, and procedures for recovering systems, infrastructure, and data after a disruptive event.

3.8. "Encryption" means the process of converting information or data into a code to prevent unauthorized access.

3.9. "Incident Response" means the organized approach to addressing and managing the aftermath of a security breach or attack.

3.10. "Integrity" means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

3.11. "Least Privilege" means the security principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations needed to perform its function.

3.12. "Multi-Factor Authentication" or "MFA" means an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

3.13. "Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

3.14. "Security Incident" means an event that potentially compromises the confidentiality, integrity, or availability of information or systems, or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

3.15. "Services" means all services provided by Smackdab to Customer pursuant to the applicable agreement between the parties.

3.16. "Smackdab" means Smackdab Inc., a Florida corporation with its principal place of business in Collier County, Florida.

3.17. "Sub-processor" means any third-party entity that processes Customer Data on behalf of Smackdab and to which Smackdab transfers Customer Data for a business purpose pursuant to a written contract.

3.18. "Vulnerability" means a weakness which can be exploited by one or more threats to gain unauthorized access to or perform unauthorized actions on a computer system or the information it contains.

4. INFORMATION SECURITY PROGRAM

4.1. Security Governance

Smackdab maintains a formal security governance structure to oversee, implement, and enforce our information security program:

- **Security Leadership:** Smackdab has appointed a Chief Information Security Officer (CISO) responsible for developing, implementing, and maintaining our security program.
- **Security Team:** A dedicated security team manages day-to-day security operations, incident response, vulnerability management, and security monitoring.
- **Executive Oversight:** Senior management review security policies, risk assessments, and major security incidents at least quarterly.
- **Security Committee:** A cross-functional security committee meets monthly to address security issues and initiatives across the organization.

4.2. Security Policies and Procedures

Smackdab maintains comprehensive written information security policies and procedures that:

- Define security roles and responsibilities
- Establish security requirements for all aspects of operations
- Specify procedures for implementing security controls
- Detail incident response protocols
- Address compliance with applicable laws and regulations
- Are reviewed and updated at least annually

4.3. Risk Management

Smackdab implements a formal risk management process that includes:

- Annual comprehensive risk assessments
- Quarterly reviews of the risk register
- Risk assessment for significant changes to systems or processes

- Clear risk acceptance criteria and escalation procedures
- Documented risk treatment plans for identified risks
- Regular reporting to executive management

4.4. Security Awareness and Training

All Smackdab personnel undergo security training and awareness activities, including:

- Security awareness training upon hire and annually thereafter
- Role-specific security training for personnel with access to sensitive systems
- Regular security updates and awareness communications
- Simulated phishing exercises to reinforce awareness
- Security requirements embedded in performance expectations

---

5. TECHNICAL SECURITY CONTROLS

5.1. Network Security

Smackdab implements multiple layers of network security controls:

- **Network Segregation:** Production networks are logically segregated from corporate networks.
- **Firewalls:** Next-generation firewalls with application-level filtering protect network boundaries.
- **Intrusion Detection/Prevention:** Network and host-based IDS/IPS monitor for and block suspicious activities.
- **DDoS Protection:** Enterprise-grade DDoS mitigation services protect against volumetric and application-layer attacks.
- **Traffic Encryption:** All data transmitted to and from Smackdab services is encrypted using TLS 1.2 or higher.
- **VPN:** Access to production environments requires secure VPN with multi-factor authentication.
- **Network Monitoring:** 24/7 monitoring of network traffic for security events and anomalies.

5.2. Access Control

Smackdab maintains strict access controls following the principles of least privilege and separation of duties:

- **Identity Management:** Centralized identity management system with documented provisioning and de-provisioning procedures.
- **Authentication Requirements:** Strong password requirements, regular password rotation, and account lockout after multiple failed attempts.
- **Multi-Factor Authentication:** MFA is required for all administrative access to production systems and is available for all Customer accounts.
- **Privileged Access Management:** Enhanced controls and monitoring for privileged accounts, with just-in-time access when possible.
- **Access Reviews:** Regular reviews of user access rights and privileges to ensure appropriate access.
- **Role-Based Access Control:** Access based on job responsibilities and need-to-know.
- **Session Management:** Automatic timeout of inactive sessions.

5.3. Endpoint Security

Smackdab protects endpoint devices used by employees and contractors:

- **Endpoint Protection:** Advanced anti-malware and endpoint detection and response (EDR) solutions.
- **Device Encryption:** Full-disk encryption for all workstations and mobile devices.
- **Mobile Device Management:** MDM solution to enforce security policies on mobile devices.
- **Patch Management:** Regular patching schedule with priority for security-related updates.
- **Secure Configuration:** Hardened baseline configurations for all endpoint types.
- **Application Control:** Controls to prevent unauthorized software installation.

5.4. Vulnerability Management

Smackdab maintains a comprehensive vulnerability management program:

- **Vulnerability Scanning:** Regular automated scanning of all systems and applications at least monthly and after significant changes.
- **Penetration Testing:** Annual penetration tests conducted by qualified independent third parties.
- **Patch Management:** Documented patch management processes with prioritization based on vulnerability severity, business impact, and exploitation risk.
- **Responsible Disclosure Program:** Public vulnerability disclosure program for external security researchers with clear submission guidelines and safe harbor provisions, subject to researchers

following program guidelines and acting in good faith without malicious intent or data exfiltration.

- **Remediation Tracking:** Formal tracking and reporting of vulnerability remediation activities with risk-based prioritization.
- **Vulnerability Risk Assessment:** Formal process to evaluate, classify, and prioritize vulnerabilities based on multiple factors including CVSS scores, exploitability, and business context.
- **Remediation Timeframes:** Risk-based approach to remediation with priorities determined by security team assessment rather than rigid timeframes.
- **Remediation Timeframes:** Target initial remediation or effective mitigation within the following timeframes after validation, subject to risk-based adjustments: Critical 7–14 days; High 30 days; Medium 60 days; Low 90 days. These targets are mirrored in the Responsible Disclosure Policy (VDP).

5.5. Malware Protection

Smackdab implements multiple layers of protection against malware:

- **Anti-Malware Solutions:** Enterprise-grade anti-malware software on all systems.
- **Email Security:** Advanced email filtering and scanning for malicious content.
- **Web Filtering:** Controls to prevent access to malicious websites.
- **Attachment Scanning:** Scanning of all file uploads for malicious content.
- **Sandboxing:** Detonation of suspicious files in isolated environments.

5.6. Logging and Monitoring

Smackdab maintains comprehensive logging and monitoring capabilities:

- **Centralized Logging:** All security-relevant logs collected in a central secure log repository.
- **Log Retention:** Security logs are retained for at least 12 months in an immutable format with integrity controls to prevent unauthorized modification.
- **Security Monitoring:** 24/7 monitoring for security events and anomalies.
- **Alert Management:** Defined alert thresholds and escalation procedures.
- **Security Information and Event Management (SIEM):** Enterprise SIEM solution for correlation and analysis of security events.
- **Continuous Monitoring:** Automated monitoring for unauthorized changes or access.

6. ORGANIZATIONAL SECURITY MEASURES

6.1. Personnel Security

Smackdab implements comprehensive personnel security measures:

- **Background Checks:** Pre-employment background checks for all employees and contractors.
- **Confidentiality Agreements:** Signed confidentiality and acceptable use agreements.
- **Security Training:** Mandatory security training during onboarding and annually thereafter.
- **Termination Procedures:** Prompt deactivation of access upon termination or role change.
- **Security Responsibilities:** Security responsibilities included in job descriptions.

6.2. Physical Security

Smackdab ensures the physical security of its facilities and equipment:

- **Data Center Security:** Production systems hosted in industry-standard data centers with SOC 2 compliance standards. Data centers maintain 24/7 security, surveillance, and environmental controls. Smackdab is currently pursuing SOC 2 Type II certification.
- **Office Security:** Physical access controls to Smackdab offices, including badge access and visitor management.
- **Equipment Security:** Secure storage and disposal of equipment containing sensitive information.
- **Clear Desk Policy:** Requirements to secure sensitive information when workstations are unattended.
- **Media Handling:** Secure handling, storage, and destruction of physical media.

6.3. Security Development Lifecycle

Smackdab integrates security throughout the software development lifecycle:

- **Secure Coding Standards:** Documented secure coding guidelines for developers.
- **Security Requirements:** Security requirements defined early in the development process.
- **Security Design Reviews:** Security architecture reviews for new features and significant changes.
- **Static Application Security Testing (SAST):** Automated code scanning for security vulnerabilities.
- **Dynamic Application Security Testing (DAST):** Runtime security testing of applications.
- **Pre-Production Security Testing:** Security testing prior to deployment to production.

- **Change Management:** Formal change management process with security review.

6.4. Configuration Management

Smackdab maintains secure configurations for all systems:

- **Hardened Baselines:** Standard secure configurations for all system types.
- **Configuration Management Database:** Inventory of all hardware and software assets.
- **Configuration Monitoring:** Continuous monitoring for unauthorized changes.
- **Secure Deployment:** Automated, secure deployment processes.
- **Environment Separation:** Strict separation between development, testing, and production environments.

---

7. DATA SECURITY

7.1. Data Classification and Handling

Smackdab classifies all data according to its sensitivity and implements appropriate controls based on classification:

- **Public Data:** Information that can be freely disclosed to the public.
- **Handling Requirements:** No special handling required
- **Examples:** Marketing materials, public documentation, press releases
- **Internal Data:** Information for internal use that does not contain sensitive details.
- **Handling Requirements:** Accessible only to authenticated Smackdab personnel
- **Examples:** General internal communications, non-sensitive operational data
- **Controls:** Basic access controls and standard protection measures
- **Confidential Data:** Sensitive business information requiring protection.
- **Handling Requirements:** Accessible only to authorized personnel with business need
- **Examples:** Customer lists, financial data, strategic plans, intellectual property
- **Controls:** Strong access controls, encryption in transit and at rest, access logging
- **Restricted Data:** Highly sensitive information requiring the strongest controls.

- **Handling Requirements:** Strictly limited access with granular permissions
- **Examples:** Authentication credentials, encryption keys, sensitive personal data
- **Controls:** Strong encryption, multi-factor authentication, enhanced monitoring, limited retention
- **Customer Data:** All data submitted by customers through the Service.
- **Handling Requirements:** Handled according to contractual obligations and data protection laws
- **Controls:** Logical separation, access controls based on principle of least privilege, encryption

7.1.1. Data Handling Procedures

For each data classification, Smackdab maintains documented procedures for:

- **Access Authorization:** Formal processes for requesting, approving, and reviewing access
- **Transmission Security:** Requirements for secure transmission based on classification
- **Storage Requirements:** Approved storage locations and encryption requirements
- **Labeling and Metadata:** Classification labeling and tagging requirements
- **Retention and Disposal:** Classification-specific retention periods and disposal methods

7.2. Customer Data Protection

Smackdab implements specific measures to protect Customer Data:

- **Data Segregation:** Logical separation of each Customer's data.
- **Access Controls:** Strict access controls for Customer Data with least privilege principles.
- **Encryption:** Encryption of Customer Data in transit and at rest.
- **Data Processing Restrictions:** Processing only as instructed by Customers.
- **Data Subject Rights:** Tools to help Customers fulfill data subject rights requests.

7.3. Data Encryption

Smackdab uses industry-standard encryption to protect data:

- **Transport Encryption:** All data in transit encrypted using TLS 1.2 or higher with modern cipher suites.
- **Storage Encryption:** Encryption of data at rest using AES-256 encryption.
- **Key Management:** Secure key management procedures including key rotation and secure storage.

- **Database Encryption:** Encryption of sensitive fields within databases.
- **Backup Encryption:** Encryption of all data backups.

7.4. Data Retention and Disposal

Smackdab implements comprehensive data lifecycle controls:

- **Retention Policies:** Defined retention periods for different data types based on:
- Legal and regulatory requirements
- Contractual obligations
- Business operational needs
- Risk assessment and data sensitivity
- **Data Return:** Upon contract termination or Customer request, Smackdab will:
- Make Customer Data available for export in standard, machine-readable formats
- Provide export tools and technical assistance as specified in the applicable agreement
- Return Customer Data within 30 days of receiving a written request
- **Data Return and Deletion Timeline:** Customer Data deletion is performed in accordance with the timelines and process outlined in our Terms of Service Section 9.5 and Data Processing Addendum Section 9. This Security Policy does not independently modify or shorten these timelines.
- Upon contract termination or expiration, Customer will have a **thirty (30) day Data Retrieval Period** to export Customer Data. After this period, Smackdab will delete Customer Data as follows:
- **Production Systems:** Customer Data will be deleted from production systems within **thirty (30) days** after the Data Retrieval Period ends
- **Backup Systems**: Customer Data will be purged from backup and archival systems no later than **ninety (90) days** after production deletion
- **Total Maximum Retention:** All Customer Data will be permanently erased from our systems within **one hundred eighty (180) days** following the end of the Data Retrieval Period
- **For Beta or preview Services:** Customer Data may be deleted **at any time without notice**, and the Data Retrieval Period and deletion timeline above **do not apply.** Beta participants are solely responsible for backing up and exporting any data they wish to retain.
- **Secure Deletion Methods:** All Customer Data deletion is performed using industry-standard methods including:

- Cryptographic erasure (where applicable)
- Digital sanitization following NIST SP 800-88 guidelines
- Verification of deletion completion
- Documentation maintained for compliance purposes
- **Media Sanitization:** Physical media containing Customer Data is sanitized before reuse or disposal using:
- Secure wiping or cryptographic erasure for digital media
- Physical destruction for media that cannot be securely wiped
- Certified destruction services for highly sensitive media
- **Deletion Verification:** Processes to verify complete deletion of data, including:
- Automated verification of deletion completion
- Documentation of deletion for compliance purposes
- Certificates of destruction upon Customer request
- **Retention Exception Process:** Formal process for handling legal holds or other retention exceptions, including:
- Legal review of all retention exception requests
- Secure preservation of only the specific data subject to the exception
- Access controls limiting visibility to authorized personnel only
- Regular review of ongoing exceptions to confirm continued validity

---

8. THIRD-PARTY RISK MANAGEMENT

8.1. Vendor Security Assessment

Smackdab evaluates the security practices of third-party service providers through a formal vendor risk management program:

- **Security Due Diligence:** Pre-engagement security assessment of all vendors who process sensitive data, including security questionnaires, documentation review, and where appropriate, technical testing.

- **Risk-Based Approach:** Level of assessment based on data sensitivity, access, and criticality to service operations, with categorization of vendors into risk tiers.
- **Ongoing Monitoring:** Regular reassessment based on risk level—annually for critical vendors, biennially for medium-risk vendors, and upon contract renewal for low-risk vendors.
- **Security Requirements:** Contractual security requirements for all service providers, including:

(i) breach notification obligations immediately and, in any event, no later than twenty-four (24) hours of discovery, to ensure Smackdab has sufficient time to analyze the incident and meet its own customer notification obligations within 48 hours;

(ii) right-to-audit provisions exercisable at least annually with 30 days notice,

(iii) security SLAs with defined penalties for non-compliance, and

(iv) obligation to flow down these requirements to subcontractors.

- **Compliance Verification:** Validation of compliance with security requirements through review of certifications, attestation reports, or direct assessments.
- **Remediation Management:** Formal process for tracking and remediating security gaps identified during vendor assessments, including risk acceptance procedures for exceptions.
- **Vendor Offboarding:** Security procedures for termination of vendor relationships, including access revocation, data return or secure deletion, and verification of contractual compliance.

8.2. Cloud Security

Smackdab implements additional controls specific to cloud environments:

- **Shared Responsibility:** Clear understanding of security responsibilities between Smackdab and cloud providers.
- **Cloud Security Configuration:** Secure configuration of cloud services and resources.
- **Cloud Security Monitoring:** Continuous monitoring of cloud environments.
- **Cloud Access Security:** Enhanced controls for cloud administrative access.
- **Cloud Vendor Assessment:** Regular security assessment of cloud service providers.

8.3. Sub-processor Management

Smackdab maintains controls over sub-processors who handle Customer Data:

- **Sub-processor Approval:** Rigorous security review before engagement.
- **Sub-processor Inventory:** Maintained and published list of sub-processors.

- **Customer Notification:** Advance notice to Customers before engaging new sub-processors.
- **Sub-processor Agreements:** Data protection terms in all sub-processor agreements.
- **Sub-processor Monitoring:** Regular review of sub-processor security practices.

---

9. INCIDENT RESPONSE

9.1. Incident Response Plan

Smackdab maintains a comprehensive incident response plan:

- **Response Team:** Dedicated incident response team with defined roles and responsibilities.
- **Response Procedures:** Documented procedures for different incident types.
- **Classification Framework:** Framework for classifying incidents by severity and type.
- **Communication Plan:** Internal and external communication procedures.
- **Regular Testing:** Annual testing of incident response procedures.
- **Post-Incident Review:** Analysis and lessons learned after incidents.

9.2. Breach Notification

Smackdab has established procedures for security breach notifications:

- **Customer Notification:** Notification to affected Customers without undue delay and in accordance with contractual and legal requirements.
- **Regulatory Notification:** Processes to identify and meet regulatory notification requirements.
- **Notification Content:** Templates and procedures for providing required information in notifications.
- **Communication Channels:** Secure and reliable methods for breach communications.
- **Documentation:** Thorough documentation of breach response activities Smackdab will notify affected Customers of a confirmed Personal-Data breach without undue delay and, in any event, within forty-eight (48) hours of awareness. For clarity, ‘Security Incident’ in the DPA is a personal-data breach under GDPR/UK GDPR. Smackdab will notify Customer within 48 hours of awareness and regulators/individuals within applicable statutory timelines (e.g., GDPR 72 hours). Regulator and individual notifications will be made in accordance with Applicable Law and Smackdab’s Privacy Policy.

9.3. Incident Detection and Response

Smackdab implements robust systems and processes to detect and respond to security incidents:

- **Security Monitoring:** 24/7 monitoring for security events and anomalies including:
- Real-time log analysis and correlation
- Network traffic analysis with anomaly detection
- Host-based intrusion detection
- User behavior analytics
- Data loss prevention alerts
- Automated suspicious activity detection
- **Alert Management and Triage:**
- Defined alert severity levels and response SLAs
- Alert correlation to reduce false positives
- Automated initial triage for known event types
- Escalation procedures based on severity
- On-call rotation for after-hours response
- **Incident Response Protocols:**
- Defined incident categories with specific playbooks
- Checklist-driven response procedures
- Secure communication channels for incident response
- Evidence preservation procedures
- Chain of custody documentation
- Timeline reconstruction tools and templates
- **Containment Strategies:**
- Predefined containment procedures by incident type
- Authorization matrix for containment actions
- Isolation procedures for affected systems

- Temporary enhanced monitoring capabilities
- Communication templates for stakeholder updates
- **Eradication and Recovery:**
- Root cause analysis methodology
- Clean-up and remediation procedures
- Business approval gates for recovery actions
- Verification testing post-recovery
- Post-incident security enhancements
- **Legal and Compliance Integration:**
- Legal team engagement protocols
- Evidence handling compliant with legal requirements
- Chain of custody documentation
- Preservation of forensic data
- Template-driven notification documentation
- **Post-Incident Analysis:**
- Formal post-incident review process
- Root cause analysis and documentation
- Lessons learned identification
- Security control enhancement recommendations
- Incident response plan updates based on findings
- Simulation exercises based on past incidents
- **Incident Metrics and Reporting:**
- Key performance indicators for incident response
- Time-to-detect and time-to-contain tracking

- Incident trends analysis
- Regular reporting to executive management
- Annual program effectiveness assessment

---

10. BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1. Business Continuity Plan

Smackdab maintains business continuity plans to ensure ongoing operations:

- **Impact Analysis:** Business impact analysis to identify critical functions and resources.
- **Recovery Strategies:** Defined strategies for different disruption scenarios.
- **Continuity Team:** Designated personnel with continuity responsibilities.
- **Communication Plan:** Procedures for emergency communications.
- **Regular Testing:** Annual testing of continuity plans.
- **Plan Maintenance:** Regular updates based on organizational changes and test results.

10.2. Disaster Recovery

Smackdab implements disaster recovery capabilities for its systems:

- **Recovery Objectives:** Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- **Backup Systems:** Redundant systems in geographically diverse locations.
- **Data Backups:** Regular backups with secure off-site storage.
- **Recovery Procedures:** Documented procedures for system recovery.
- **Recovery Testing:** Regular testing of recovery procedures.
- **Failover Capabilities:** Automated or rapid manual failover for critical systems.

10.3. Resilience and Service Continuity

Smackdab designs its systems and operations for high resilience and service continuity:

- **System Redundancy:** Redundant infrastructure components to eliminate single points of failure, including:
- Redundant network connectivity and routing

- Redundant power systems with UPS and generator backup
- Clustered server configurations and load balancing
- Redundant storage systems with real-time replication
- **High Availability Design:** High-availability architecture for critical systems, featuring:
- Active-active configurations where feasible
- Automated failover capabilities
- Geographic distribution across multiple availability zones
- Service levels as specified in the applicable Service Level Agreement
- **Load Balancing:** Distribution of workloads across multiple resources to optimize performance and availability:
- Application load balancing
- Network traffic distribution
- Database query distribution
- Automatic scaling based on demand
- **Fault Tolerance:** Systems designed to continue functioning despite component failures:
- Graceful degradation capabilities
- Circuit breakers to prevent cascading failures
- Retry logic with exponential backoff
- Health checks with automated recovery procedures
- **Performance and Capacity Management:**
- Continuous monitoring of system performance and capacity
- Proactive capacity planning based on growth projections
- Performance testing to ensure scalability
- Resource utilization thresholds with automated alerts
- **Dependency Management:**

- Inventory of critical dependencies (internal and external)
- Contingency plans for key third-party service disruptions
- Architectural design to minimize impact of dependency failures
- Regular testing of dependency failure scenarios
- **Business Impact Analysis:**
- Regular assessment of critical business functions
- Prioritization of recovery for key services
- Recovery objectives established based on business impact analysis and as defined in applicable service agreements
- Business continuity requirements driving technical architecture decisions

---

11. LEGAL COMPLIANCE

11.1. Regulatory Landscape

Smackdab maintains a compliance program designed to address requirements from multiple regulatory frameworks affecting our operations and the processing of Customer Data, including but not limited to:

- **General Data Protection Laws:** GDPR (EU), UK GDPR, CCPA/CPRA (California), CDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), UCPA (Utah)
- **Sector-Specific Regulations:** HIPAA (healthcare), GLBA (financial services), FERPA (education)
- **International Standards:** ISO 27001, ISO 27701, NIST Cybersecurity Framework
- **Industry Standards:** PCI DSS (for payment processing), OWASP Application Security Verification Standard

11.2. Compliance Program

Smackdab's compliance program includes:

- **Compliance Mapping:** Comprehensive mapping of security controls to multiple regulatory frameworks
- **Regulatory Monitoring:** Regular tracking of changes to applicable laws and regulations
- **Impact Assessments:** Formal process for evaluating the impact of regulatory changes
- **Compliance Governance:** Defined roles and responsibilities for compliance management

- **Documentation Management:** Maintenance of evidence demonstrating compliance
- **Compliance Reporting:** Regular internal reporting on compliance status
- **Remediation Management:** Process for addressing compliance gaps

11.3. Legal Requirements

Smackdab designs security controls to meet legal requirements for:

- **Security Measures:** Implementation of appropriate technical and organizational security measures
- **Data Subject Rights:** Support for individual rights regarding personal data
- **Breach Notification:** Timely notification of security incidents as required by law
- **Cross-Border Data Transfers:** Appropriate safeguards for international data transfers
- **Vendor Management:** Oversight of third parties processing data on our behalf
- **Documentation:** Maintenance of required documentation, including Records of Processing Activities

11.4. International Compliance

For operations across multiple jurisdictions, Smackdab:

- **Monitors Regional Requirements:** Tracks jurisdiction-specific security and privacy requirements
- **Implements Country-Specific Controls:** Adds controls as needed for country-specific requirements
- **Provides Territory-Specific Terms:** Offers supplementary terms for specific jurisdictions
- **Addresses Data Residency:** Offers regional data hosting options for customers with data localization requirements
- **Documents Transfer Mechanisms:** Maintains documentation of cross-border transfer mechanisms

---

12. COMPLIANCE AND CERTIFICATIONS

12.1. Regulatory Compliance

Smackdab maintains compliance with applicable laws and regulations:

- **Data Protection Laws:** Compliance with relevant data protection regulations (e.g., GDPR, CCPA, CPRA).
- **Industry Regulations:** Compliance with applicable industry-specific regulations.

- **Compliance Monitoring:** Continuous monitoring for compliance with legal requirements.
- **Compliance Documentation:** Maintenance of evidence demonstrating compliance.
- **Regulatory Updates:** Monitoring for changes in regulatory requirements.

12.2. Security Certifications and Attestations

Smackdab maintains the following security certifications and attestations:

- **SOC 2 Type II:** Annual SOC 2 Type II examination covering Security, Availability, and Confidentiality trust service criteria.
- **ISO 27001:** Certification of Information Security Management System (in process, expected completion Q4 2025).
- **EU-US Data Privacy Framework:** Participates in and has self-certified to the EU-US Data Privacy Framework for EU-US data transfers.
- **Data Privacy Framework:** Compliance with EU-US Data Privacy Framework principles.
- **CSA STAR:** Registration in the Cloud Security Alliance Security Trust Assurance and Risk (STAR) program.

12.3. Contractual Compliance

Smackdab implements measures to maintain compliance with contractual obligations:

- **Customer Agreements:** Monitoring compliance with customer security requirements.
- **Data Processing Agreements:** Implementation of data processing terms.
- **Service Level Agreements:** Processes to meet service level commitments.
- **Audit Rights:** Support for customer audit rights as specified in agreements.
- **Reporting Requirements:** Processes to fulfill contractual reporting obligations.

---

13. SECURITY AUDITS AND ASSESSMENTS

13.1. Internal Audits

Smackdab conducts regular internal security audits:

- **Audit Program:** Documented internal audit program covering all security domains.
- **Audit Schedule:** Annual schedule of internal security audits.

- **Audit Methodology:** Consistent methodology for conducting audits.
- **Findings Management:** Process for tracking and remediating audit findings.
- **Management Reporting:** Regular reporting of audit results to senior management.

13.2. External Assessments

Smackdab engages independent third parties to assess its security:

- **Annual Penetration Testing:** Comprehensive penetration tests of applications and infrastructure.
- **Vulnerability Assessments:** Regular vulnerability assessments of systems and applications.
- **Compliance Audits:** Independent audits for regulatory and certification compliance.
- **Security Control Assessments:** Periodic assessment of security control effectiveness.
- **Social Engineering Tests:** Simulated phishing and other social engineering tests.

13.3. Continuous Monitoring

Smackdab implements continuous security monitoring:

- **Automated Scanning:** Regular automated security scanning of systems and applications.
- **Configuration Monitoring:** Continuous monitoring for secure configurations.
- **Threat Intelligence:** Integration of threat intelligence into security monitoring.
- **Security Metrics:** Tracking and analysis of security performance metrics.
- **Security Dashboards:** Real-time visibility into security status.

---

14. UPDATES TO THIS POLICY

14.1. Policy Maintenance

This Security Policy is reviewed and updated at least annually and more frequently when necessary to address:

- Changes in business practices or technology infrastructure
- Results of security assessments and audits
- Changes in the threat landscape or emerging security risks
- Evolving legal and regulatory requirements

- Feedback from customers and security partners
- Lessons learned from security incidents

All changes to this Policy must be approved by senior management and reviewed by the Security Committee before implementation.

14.2. Change Notification

Smackdab reserves the right to modify this Security Policy at any time. We will provide notice of changes as follows:

- **Material Changes:** For significant changes that substantially affect security practices or customer obligations, we will provide at least 30 days' advance notice via:
- Email to the primary contact for each customer account
- Notification in the Service administrative interface
- Updated version posted on our website with change summary
- **Non-Material Changes:** For minor updates, clarifications, or corrections that do not substantially affect security practices, we will:
- Post the updated version on our website
- Update the "Last Updated" date
- Maintain change logs accessible to customers

Material changes to this Policy will become effective 30 days after posting unless otherwise specified. Your continued use of the Service after the effective date constitutes your acceptance of the revised Policy.

Smackdab will not implement modifications that materially reduce the security or privacy protections applicable to Customer Data during an active Subscription Term.

14.3. Version History

Smackdab maintains a complete version history of this Policy, including all prior versions and a detailed change log. Customers may request access to this version history by contacting their account representative or security@smackdab.ai.

We encourage you to periodically review this Policy to stay informed about our security practices.

---

15. CONTACT INFORMATION

If you have questions about our security practices or this Policy, please contact us:

Email: security@smackdab.ai **Mail:** Smackdab Inc. Attn: Security Team 372 Live Oak Ln Marco Island, FL 34145 United States **Phone:** +1 (239) 299-4616

For reporting security vulnerabilities, please email: security@smackdab.ai

This PDF is the formal downloadable version of SECURITY POLICY.