SMACKDAB INC. OFFICIAL POLICY

EMPLOYEE DATA HANDLING POLICY

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

DATA CLASSIFICATION AND PROTECTION POLICY

Effective Date: February 20, 2026

Last Updated: August 14, 2026

Version:

1.0

Document Location: https://smackdab.ai/legal/employee-data-handling-policy/

1. INTRODUCTION AND PURPOSE

1.1. Overview

This Data Classification and Protection Policy ("Policy") establishes the framework by which Smackdab Inc. ("Smackdab," "Company," "we," "us," or "our") identifies, classifies, and protects all sensitive data created, processed, stored, and transmitted by the Smackdab platform and its supporting systems. This Policy is a foundational element of Smackdab's information security program and is designed to satisfy the requirements of the Cloud Application Security Assessment (CASA) framework, which is built upon the OWASP Application Security Verification Standard (ASVS)

4.0. Specifically, this Policy addresses the following OWASP ASVS requirements:

ASVS Ref

Requirement

Coverage

V1.8.1

Verify that all sensitive data is identified and classified into protection levels.

Section 3

V1.8.2

Verify that all protection levels have an associated set of protection requirements (encryption, integrity, retention, privacy, confidentiality) applied in the architecture.

Section 4

V8.3.4

Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data.

Sections 3–6

V8.1.1

Verify the application protects sensitive data from being cached in server components.

Section 5.4

V8.1.2

Verify that cached or temporary copies of sensitive data are protected or purged after use.

Section 5.4

V8.2.1

Verify that sensitive data is sent to the server in the HTTP message body or headers, not query strings.

Section 5.3

V8.2.2

Verify that data in browser storage does not contain sensitive data.

Section 5.3

V8.3.1

Verify that sensitive data is sent to the server in the HTTP message body or headers.

Section 5.3

V8.3.3

Verify that users have a method to remove or export their data on demand.

Section 6.3

V8.3.5

Verify accessing sensitive data is audited (without logging the sensitive data itself).

Section 7

V8.3.7

Verify that sensitive data that is required to be encrypted, is encrypted using approved algorithms.

Section 5.2

V8.3.8

Verify that sensitive personal information is subject to data retention classification.

Section 6

1.2. Purpose

The purpose of this Policy is to:

(a) Ensure that all sensitive data created, processed, stored, and transmitted by the Smackdab platform is identified and classified into defined protection levels (ASVS V1.8.1, V8.3.4);

(b) Define protection requirements for each classification level, including encryption, integrity, retention, privacy, and confidentiality controls (ASVS V1.8.2);

(c) Establish data handling procedures that govern the full data lifecycle from creation through secure disposal;

(d) Ensure compliance with applicable Data Protection Laws, including GDPR, CCPA/CPRA, VCDPA, CPA, CTDPA, UCPA, and sector-specific regulations;

(e) Support Smackdab's CASA certification and ongoing compliance with the OWASP ASVS 4.0 framework; and

(f) Provide a reference document for auditors, assessors, customers, and internal stakeholders.

1.3. Scope

This Policy applies to all data processed by the Smackdab platform, including but not limited to Customer Data, Personal Data, Confidential Information, and internal business data. It covers all environments (production, staging, development, disaster recovery, and backup), all personnel (employees, contractors, consultants, and third-party service providers), and all systems, applications, APIs, mobile applications, and infrastructure operated by or on behalf of Smackdab. This Policy supplements and should be read in conjunction with the following Smackdab legal and security documents:

- **Terms of Service (TOS):**https://smackdab.ai/legal/terms-of-service
- **Data Processing Addendum (DPA):**https://smackdab.ai/legal/data-processing-addendum
- **Security Policy:**https://smackdab.ai/legal/security-policy
- **Employee Data Handling Policy:**https://smackdab.ai/legal/employee-data-handling-policy
- **Privacy Policy:**https://smackdab.ai/legal/privacy-policy
- **Sub-processor List:**https://smackdab.ai/legal/sub-processors

1.4. Authority and Governance

This Policy is owned by the Chief Information Security Officer (CISO) and approved by Smackdab's Executive Leadership. The CISO is responsible for the implementation, maintenance, and enforcement of this Policy. The cross-functional Security Committee reviews this Policy at least annually and recommends

updates as necessary. The Data Protection Officer (DPO) provides advisory oversight to ensure alignment with applicable Data Protection Laws.

---

2. DEFINITIONS

The following definitions apply to this Policy.

Terms not defined herein shall have the meanings assigned in the Smackdab Terms of Service (TOS) or the Data Processing Addendum (DPA).

These definitions are consistent with and aligned to the definitions used across all Smackdab legal and security documents.

2.1. "Applicable Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data, including but not limited to the GDPR, UK GDPR, CCPA, CPRA, VCDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), UCPA (Utah), and any related regulations. (Aligned: DPA §1.1; Employee Data Handling Policy §3.8)

2.2. "Client Data" or "Customer Data" means all electronic data, text, messages, communications, information, documents, files, images, graphics, audio, video, or other materials submitted to, stored in, processed by, or transmitted through the Services by Customer, its Affiliates, or Authorized Users acting on Customer’s behalf. (Aligned: TOS; DPA §1.2; Security Policy §3.5; Employee Data Handling Policy §3.3)

2.3. "Confidential Information" means non-public information that is designated as confidential or that a reasonable person would understand to be confidential given the nature of the information and the circumstances of disclosure.

Confidential Information includes, but is not limited to, Customer Data, trade secrets, business plans, financial information, source code, and technical specifications. (Aligned: Employee Data Handling Policy §3.1)

2.4. "Data Breach" or "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored, or otherwise processed by Smackdab. (Aligned: DPA §1.11; Security Policy §3.6, §3.14; Employee Data Handling Policy §3.4)

2.5. "Data Classification" means the process of categorizing data based on its sensitivity, value, regulatory requirements, and criticality to Smackdab and its Customers. (Aligned: Employee Data Handling Policy §3.5)

2.6. "Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data (typically the Client). (Aligned: DPA §1.4)

2.7. "Data Processor" means the entity which Processes

Personal Data on behalf of the Data Controller (typically Smackdab when Processing Client Data). (Aligned: DPA §1.5)

2.8. "Data Subject" means the identified or identifiable natural person to whom Personal Data relates. (Aligned: DPA §1.6)

2.9. "Encryption" means the process of converting information or data into a code to prevent unauthorized access, using industry-standard algorithms and key lengths. (Aligned: Security Policy §3.8)

2.10. "Personal Data" means any information relating to an identified or identifiable natural person contained within Client Data, processed by Smackdab on behalf of Client pursuant to the Agreement. (Aligned: DPA §1.9; Security Policy §3.13; Employee Data Handling Policy §3.10)

2.11. "Processing" means any operation performed on data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, restriction, erasure, or destruction.

(Aligned: DPA §1.10; Employee Data Handling Policy §3.11)

2.12. "Protection Level" means a defined tier of security controls, handling requirements, and safeguards applied to data based on its classification.

2.13. "Sensitive Data" means special categories of Personal Data as defined under applicable Data Protection Laws, including data revealing racial or ethnic origin, political opinions, religious beliefs, genetic data, biometric data, health data, data concerning sex life or sexual orientation, financial account information, government-issued identification numbers, and credentials. (Aligned: Employee Data Handling Policy §3.13; DPA §2.3)

2.14. "Services" means all subscription-based software and related services provided by Smackdab under the Terms of Service. (Aligned: Security Policy §3.15)

2.15. "Sub-processor" means any third-party entity that processes Customer Data on behalf of Smackdab pursuant to a written contract. (Aligned: DPA §1.14; Security Policy

§3.17)

---

3. DATA CLASSIFICATION FRAMEWORK

In accordance with OWASP ASVS V1.8.1 and V8.3.4, Smackdab has identified all sensitive data created and processed by the application and classified it into defined protection levels. This classification framework is the foundation upon which all data handling, encryption, access control, retention, and disposal requirements are built. This framework is consistent with the data classification levels defined in the Smackdab Security Policy (§2.2, §7.1) and the Employee Data Handling Policy (§5.1).

3.1. Classification Levels

Smackdab classifies all data into five (5) protection levels, ordered from lowest to highest sensitivity:

Level

Classification

Description

Examples

PL-1

Public

Information explicitly approved for public disclosure that poses no risk if disclosed.

Marketing materials, public documentation, press releases, public website content, published API docs

PL-2

Internal

Non-sensitive information for internal Smackdab use that does not contain personal data or confidential business details.

General internal communications, non-sensitive operational data, organizational charts, internal meeting agendas

PL-3

Confidential

Sensitive business information requiring protection, including non-public financial data, strategic information, and business-critical intellectual property.

Customer lists, financial data, strategic plans, intellectual property, source code, product roadmaps, vendor agreements, non-public API specifications

PL-4

Customer Data

All data submitted by Customers through the Services, which may include Personal Data and confidential business information. Processing is governed by contractual obligations (TOS, DPA) and Applicable Data Protection Laws.

CRM records, contact information, communication logs, marketing interaction data, user credentials, financial information processed via Smackdab Pay, any data uploaded or created by Customers

PL-5

Restricted

Highly sensitive information requiring the strongest controls, including Sensitive Data (special categories of Personal Data), authentication credentials, encryption keys, and data subject to heightened regulatory requirements.

Authentication credentials, encryption keys, sensitive personal data (health, biometric, financial account numbers), government-issued IDs, PHI (when BAA in place), data subject to HIPAA/PCI DSS

3.2. Data Inventory and Identification

Smackdab maintains a comprehensive data inventory that maps all categories of data processed by the platform to their assigned classification levels. The data inventory includes:

(a) A catalog of all data types processed by the Smackdab platform, including data types within Customer Data that are determined and controlled by the Client in its sole discretion (DPA §2.3);

(b) The source and destination of each data type, including internal systems, third-party integrations, and Sub-processors;

(c) The assigned classification level (PL-1 through PL-5) for each data type;

(d) The applicable regulatory and contractual requirements for each data type;

(e) The data owner responsible for maintaining the classification; and

(f) The retention period applicable to each data type (see Section 6). The data inventory is reviewed and updated at least annually and upon any material change to the Services, data processing activities, or regulatory landscape.

3.3. Classification Responsibility

Data classification responsibility is assigned as follows: **Data Owners:** Responsible for the initial classification of data within their domain and for reviewing the classification at least annually. **Information Security Team:** Responsible for maintaining the classification framework, providing guidance on classification decisions, and auditing classifications for accuracy. **CISO:** Responsible for approving the overall classification framework and resolving classification disputes. **Customers (for Customer Data):** Clients determine and control the types of Personal Data submitted to the Services and are responsible for ensuring that data is appropriate for processing within the Services (DPA §2.3). Clients are instructed not to store Special Categories of Personal Data in standard service fields except where explicitly permitted by Smackdab (DPA §2.3).

3.4. Reclassification

Data may be reclassified when circumstances change, including changes in regulatory requirements, contractual obligations, business needs, or when aggregation of data elements creates a higher sensitivity level than individual elements. Reclassification follows the same approval process as initial classification. When in doubt, data shall be classified at the higher protection level until properly assessed.

---

4. PROTECTION REQUIREMENTS BY CLASSIFICATION LEVEL

In accordance with OWASP ASVS V1.8.2, each classification level (protection level) has an associated, documented set of protection requirements encompassing encryption, integrity, retention, privacy, access control, and other confidentiality requirements. These requirements are applied consistently across the Smackdab architecture. The following table provides the complete protection requirement matrix:

4.1. Encryption Requirements

Requirement

PL-1 Public

PL-2 Internal

PL-3 Confidential

PL-4 Customer Data

PL-5 Restricted

Encryption in Transit

Optional (HTTPS preferred)

TLS 1.2+

TLS 1.2+ (required)

TLS 1.2+ (required)

TLS 1.2+ with modern cipher suites (required)

Encryption at Rest

Not required

Not required

AES-256 (required)

AES-256 (required)

AES-256 with per-tenant or per-field encryption

Database Field Encryption

N/A

N/A

Selective (sensitive fields)

Selective (sensitive fields)

Required for all sensitive fields

Backup Encryption

N/A

Standard

AES-256 (required)

AES-256 (required)

AES-256 (required)

Key Management

N/A

Standard

NIST SP 800-57 compliant

NIST SP 800-57 compliant; key rotation

NIST SP 800-57; HSM-backed; strict key rotation

Reference: Security Policy §7.3 (Data Encryption); OWASP ASVS V6.1, V6.2, V8.3.7.

4.2. Access Control Requirements

Requirement

PL-1 Public

PL-2 Internal

PL-3 Confidential

PL-4 Customer Data

PL-5 Restricted

Authentication

None

Standard auth

Strong auth

Strong auth + RBAC

MFA required

Authorization Model

Open access

Authenticated users

Role-based (need-to-know)

Least privilege + logical tenant separation

Granular permissions; just-in-time access

Access Reviews

N/A

Annual

Quarterly

Quarterly

Monthly

Access Logging

N/A

Basic

Detailed (required)

Detailed (required)

Enhanced with alerting

Privileged Access

N/A

Standard controls

Enhanced controls

Enhanced controls; logged sessions

PAM; JIT access; dual approval

Reference: Security Policy §5.2 (Access Control); Employee Data Handling Policy §6 (Access Control).

4.3. Integrity Requirements

Requirement

PL-1 Public

PL-2 Internal

PL-3 Confidential

PL-4 Customer Data

PL-5 Restricted

Input Validation

Standard

Standard

Strict validation

Strict validation

Strict validation + integrity checks

Change Detection

N/A

Standard logging

Tamper detection

Tamper detection + audit trail

Cryptographic integrity verification

Backup Integrity

N/A

Standard

Verified checksums

Verified checksums

Verified checksums + immutable backups

Data Validation

N/A

Basic

Schema validation

Schema validation

Schema validation + integrity hashing

4.4. Privacy and Confidentiality Requirements

Requirement

PL-1 Public

PL-2 Internal

PL-3 Confidential

PL-4 Customer Data

PL-5 Restricted

Data Minimization

N/A

Recommended

Required

Required

Strictly required

Purpose Limitation

N/A

Internal use only

Specified purposes

Per DPA §2.2 instructions only

Strictly limited; documented

Anonymization / Pseudonymization

N/A

N/A

Where feasible

Where feasible for analytics

Required for non-production use

Data Masking in UI

N/A

N/A

Selective

Selective masking

Default masking; unmasking requires explicit action

Logical Separation

N/A

N/A

Departmental separation

Tenant-level logical separation

Enhanced isolation; dedicated controls

Confidentiality Agreements

N/A

Employment terms

NDA required

NDA + DPA required

Enhanced NDA + specific access agreements

Reference: DPA §2.2 (Client Instructions); DPA §4.2 (Confidentiality); Security Policy §7.2 (Customer Data Protection).

4.5. Retention Requirements

Detailed retention periods are specified in Section 6 of this Policy. At a summary level:

Classification

Default Retention

Disposal Method

PL-1 Public

Indefinite (unless superseded)

Standard deletion

PL-2 Internal

Per business need; maximum 3 years after last use

Secure deletion

PL-3 Confidential

Per legal/contractual requirement; reviewed annually

NIST SP 800-88 compliant secure deletion

PL-4 Customer Data

Duration of Agreement + 180 days (DPA §9; TOS); or upon Client written request

NIST SP 800-88; cryptographic erasure; certification available within 30 days

PL-5 Restricted

Minimum necessary; strict time limits; reviewed quarterly

NIST SP 800-88; cryptographic erasure; physical destruction where applicable

Reference: DPA §9 (Deletion or Return of Personal Data); Security Policy §7.4 (Data Retention and Disposal); OWASP ASVS V8.3.8.

5. TECHNICAL PROTECTION CONTROLS

This section details the specific technical controls implemented to protect data in accordance with the protection requirements defined in Section 4. These controls are aligned with the Smackdab Security Policy (§5) and address specific OWASP ASVS verification requirements.

5.1. Transport Layer Security

All data transmitted to and from Smackdab Services is encrypted using TLS 1.2 or higher with modern cipher suites (Security Policy §5.1). This includes all API communications, web interface traffic, mobile application data, inter-service communications between components, and data transfers to and from Sub-processors. Deprecated or insecure protocols (SSL 2.0/3.0, TLS 1.0/1.1) are disabled. Certificate pinning is implemented for mobile applications where supported.

5.2. Encryption at Rest

All Customer Data (PL-4), Confidential Data (PL-3), and Restricted Data (PL-5) is encrypted at rest using AES-256 encryption (Security Policy §7.3). This applies to primary database storage, file storage and object storage, backup systems (with separate encryption keys), and temporary processing storage. Key management follows NIST SP 800-57 guidelines, including regular key rotation, separation of duties for key administration, secure key storage (HSM for PL-5 data), and key lifecycle management including generation, distribution, storage, rotation, revocation, and destruction. This control satisfies OWASP ASVS V8.3.7: sensitive data required to be encrypted is encrypted using approved algorithms providing both confidentiality and integrity.

5.3. Client-Side Data Protection

In accordance with OWASP ASVS V8.2.1, V8.2.2, and V8.3.1, the Smackdab application implements the following client-side data protection controls: **Sensitive Data in HTTP Parameters:** Sensitive data is transmitted only in HTTP message bodies or headers. Sensitive data, API keys, session tokens, and authentication credentials are never included in URL query string parameters. **Browser Storage:** Sensitive data is not stored in browser storage mechanisms (localStorage, sessionStorage, IndexedDB). Session identifiers may be stored in secure, HttpOnly, SameSite cookies with appropriate expiration. **Cache Controls:** Responses containing sensitive data include appropriate anti-caching HTTP response headers (Cache-Control: no-store, no-cache, must-revalidate; Pragma: no-cache) to prevent sensitive data from being cached in browsers (ASVS V8.2.3).

5.4. Server-Side Caching Protection

In accordance with OWASP ASVS V8.1.1 and V8.1.2, the following server-side caching controls are implemented:

(a) Sensitive data is protected from being cached in server components such as load balancers, CDN nodes, and application-level caches;

(b) All cached or temporary copies of sensitive data are protected from unauthorized access and are purged or invalidated after the authorized user accesses the sensitive data;

(c) Caching mechanisms are configured to only cache responses with correct content types and which do not contain sensitive, dynamic content;

(d) Request parameters are minimized to reduce the risk of data exposure through hidden fields, AJAX variables, cookies, and header values (ASVS V8.1.3); and

(e) The application detects and alerts on abnormal numbers of requests by IP, user, or other criteria to guard against bulk data extraction (ASVS V8.1.4).

5.5. Memory Protection

Sensitive information contained in memory is overwritten as soon as it is no longer required to mitigate memory dumping attacks. This is accomplished through secure memory handling practices in the application code, automatic garbage collection with secure overwrite for sensitive objects, and avoidance of unnecessary copies of sensitive data in memory. This control satisfies OWASP ASVS V8.3.6.

5.6. Logging and Audit Controls

In accordance with OWASP ASVS V8.3.5, all access to sensitive data is audited. Audit logs record the user identity, timestamp, data accessed (by reference, not content), action performed, and source IP and session information. Critically, the actual sensitive data values are never written to log files. Logs are stored in a centralized, immutable log repository and retained for at least twelve (12) months (Security Policy §5.6). Automated monitoring and alerting is configured for anomalous access patterns to sensitive data.

---

6. DATA LIFECYCLE MANAGEMENT

This section establishes the controls governing data throughout its lifecycle, from creation and collection through processing, storage, retention, and ultimate secure disposal. These controls satisfy OWASP ASVS V8.3.8 (data retention classification for sensitive personal information).

6.1. Data Collection and Creation

Data collection and creation are governed by the principles of data minimization and purpose limitation:

(a) Only the minimum data necessary for the specified, explicit, and legitimate purpose is collected or created;

(b) The purpose of collection is documented in the data inventory and privacy notices;

(c) Where Customer Data is involved, processing occurs only in accordance with Client's documented lawful instructions (DPA §2.2); and

(d) Clients are solely responsible for ensuring a valid lawful basis for processing and for providing necessary privacy notices and obtaining required consents (DPA §3).

6.2. Data Retention Schedule

The following retention schedule applies. Retention periods are determined based on legal and regulatory requirements, contractual obligations, business operational needs, and risk assessment and data sensitivity (Security Policy §7.4):

Data Category

Classification

Retention Period

Legal Basis / Reference

Customer Data (active account)

PL-4

Duration of Agreement

TOS; DPA §2.3

Customer Data (post-termination)

PL-4

Up to 180 days, then secure deletion

DPA §9; TOS

Customer Data (upon written request)

PL-4

Deleted per DPA; certification within 30 days

DPA §9

Customer Data in backups

PL-4

Removed per backup rotation (typically 90 days)

Security Policy §7.4

Personal Data (Data Subject requests)

PL-4/PL-5

Per applicable Data Protection Law deadlines

GDPR Art. 17; CCPA; DPA §4.5

Authentication credentials

PL-5

Active period only; rotated per policy

Security Policy §5.2

Encryption keys

PL-5

Per NIST SP 800-57 key lifecycle

Security Policy §7.3

Security logs and audit trails

PL-3

Minimum 12 months in immutable format

Security Policy §5.6

Internal operational data

PL-2

Per business need; max 3 years

Internal policy

Public content

PL-1

Indefinite (until superseded)

N/A

Financial records

PL-3/PL-5

Per applicable law (typically 7 years)

GAAP; tax regulations

Employee HR data

PL-3/PL-5

Per applicable employment law

Employment law; Employee Data Handling Policy

6.3. Data Subject Rights and Data Portability

In accordance with OWASP ASVS V8.3.3, users have the ability to remove or export their data on demand: **Data Export:** Smackdab provides tools within the Services for Customers to export their Customer Data in

standard, machine-readable formats (Security Policy §7.4). Upon request, Smackdab will return Customer Data within 30 days in an industry-standard format with written certification of completion. **Data Deletion:** Customers may request deletion of their data at any time. Smackdab will securely delete Customer Data in accordance with the DPA (§9) and provide written certification of deletion within 30 days of completion of the deletion process. **Data Subject Requests:** Smackdab provides reasonable assistance to Clients in fulfilling Data Subject requests (access, rectification, erasure, portability, restriction, objection) as required by Applicable Data Protection Laws (DPA §4.5). Requests received directly from Data Subjects are promptly forwarded to the relevant Client.

6.4. Secure Data Disposal

When data reaches the end of its retention period or upon valid deletion request, Smackdab implements secure disposal using the following methods (Security Policy §7.4):

(a) Cryptographic erasure (where applicable) by destroying the encryption keys used to protect the data;

(b) Digital sanitization following NIST SP 800-88 guidelines;

(c) Logical deletion from production environments within 30 days, with verification and documentation maintained for 7 years;

(d) Removal from backup systems according to backup rotation schedule (typically 90 days); and

(e) Physical destruction for media that cannot be securely wiped, using certified destruction services. Deletion verification processes include automated verification of deletion completion, documentation of deletion for compliance purposes, and certificates of destruction upon Customer request.

6.5. Retention Exception Process

Exceptions to the standard retention schedule (e.g., legal holds) follow a formal process that includes 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, and regular review of ongoing exceptions to confirm continued validity (Security Policy §7.4).

---

7. MONITORING, AUDITING, AND COMPLIANCE

7.1. Continuous Monitoring

Smackdab implements continuous monitoring to verify that data classification and protection controls are operating effectively. This includes 24/7 security monitoring with SIEM for security events and anomalies (Security Policy §5.6), automated data loss prevention (DLP) controls to detect and prevent unauthorized data exfiltration, user behavior analytics to identify anomalous data access patterns, and real-time alerting for policy violations including unauthorized access attempts and bulk data extraction.

7.2. Audit Program

Compliance with this Policy is verified through internal audits conducted at least annually, external assessments by qualified independent third parties (Security Policy §13.2), penetration testing performed annually by independent third parties (Security Policy §5.4), vulnerability assessments conducted at least monthly and after significant changes (Security Policy §5.4), and SOC 2 Type II examinations covering Security, Availability, and Confidentiality (Security Policy §12.2). Customers may exercise their audit rights as specified in the DPA (§4.7), including requesting information necessary to demonstrate compliance, conducting or mandating third-party audits (subject to confidentiality and non-competition requirements), and requesting relevant third-party audit reports (e.g., SOC 2 Type II).

7.3. CASA Compliance

This Policy is a key compliance artifact for Smackdab's Cloud Application Security Assessment (CASA) certification. The CASA assessment, built upon the OWASP ASVS 4.0 framework, evaluates Smackdab's security controls across fourteen categories including architecture, data protection, and cryptography. Smackdab undergoes annual CASA revalidation and maintains evidence of compliance with all applicable ASVS requirements. The ASVS compliance mapping in Section 1.1 provides a detailed cross-reference between specific ASVS requirements and the sections of this Policy that address them.

7.4. Regulatory Compliance

This Policy supports compliance with the following regulatory frameworks: **GDPR/UK GDPR:** Data classification supports Article 5 (data processing principles), Article 25 (data protection by design and default), Article 30 (records of processing activities), and Article 32 (security of processing). **CCPA/CPRA:** Classification of Personal Information supports Smackdab's obligations as a Service Provider (DPA §7), including restrictions on selling/sharing, purpose limitation, and consumer rights support. **ISO 27001:** This Policy implements Annex A controls including A.5.12 (Classification of information), A.5.13 (Labelling of information), A.5.10 (Acceptable use of information), and A.8.10 (Information deletion). **SOC 2:** Data classification supports the Common Criteria for the Security, Availability, and Confidentiality trust service categories. **HIPAA:** For customers with executed BAAs, PL-5 controls apply to PHI as required (DPA §8).

---

8. THIRD-PARTY AND SUB-PROCESSOR DATA HANDLING

Smackdab ensures that data classification and protection requirements extend to all third parties and Sub-processors that process data on Smackdab's behalf.

8.1. Sub-Processor Requirements

All Sub-processors engaged by Smackdab are subject to the following requirements (DPA §4.4; Security Policy §8):

(a) Pre-engagement security assessment through Smackdab's formal vendor risk management program;

(b) Written data protection agreements imposing obligations substantially similar to those in the DPA;

(c) Contractual requirements including breach notification within 24 hours, right-to-audit provisions, security SLAs, and flow-down requirements to subcontractors (Security Policy §8.1);

(d) Ongoing monitoring based on risk level (annual for critical vendors, biennial for medium-risk);

(e) Customer notification prior to engaging new Sub-processors, with a 30-day objection period (DPA §4.4); and

(f) Secure vendor offboarding including access revocation and data return or deletion (Security Policy §8.1). The current list of Sub-processors is published at https://smackdab.ai/legal/sub-processors (DPA §4.4).

8.2. International Data Transfers

Where data is transferred internationally, Smackdab implements appropriate transfer mechanisms including EU Standard Contractual Clauses (SCCs) for EEA/UK/Swiss transfers (DPA §6.2), the UK Addendum for UK GDPR transfers, EU-US Data Privacy Framework certification (Security Policy §12.2), and appropriate adaptations for Swiss transfers under the Swiss Federal Data Protection Act (DPA §6.2). All international transfers are documented and subject to the same classification-based protection requirements defined in this Policy.

---

9. ROLES AND RESPONSIBILITIES

The following roles and responsibilities govern the implementation of this Policy. These are consistent with and supplement the roles defined in the Employee Data Handling Policy (§4) and Security Policy (§4.1):

Role

Responsibilities

CISO

Owns this Policy. Approves classification framework. Oversees implementation. Resolves classification disputes. Reports to Executive Leadership.

Data Protection Officer (DPO)

Monitors compliance with Data Protection Laws. Advises on DPIAs. Liaison with supervisory authorities. Ensures alignment with DPA obligations.

Information Security Team

Maintains data inventory. Implements and monitors technical controls. Audits classifications. Investigates incidents. Manages vulnerability and patch programs.

Legal and Compliance Team

Advises on regulatory requirements. Reviews contractual obligations. Supports Data Subject request responses. Reviews data transfer mechanisms.

Engineering and Development

Implements technical controls in application code. Follows secure development lifecycle. Ensures data protection by design and default.

Customer Support

Accesses Customer Data only as authorized for legitimate support purposes. Logs all access. Forwards Data Subject requests to Clients.

All Personnel

Complies with this Policy. Completes required training. Reports incidents. Handles data per its classification level. Maintains confidentiality.

Customers (Data Controllers)

Determine types of Personal Data submitted. Ensure lawful basis for processing. Provide privacy notices and obtain consents. Instruct Smackdab on processing.

---

10. DATA CLASSIFICATION INCIDENT RESPONSE

Security Incidents affecting classified data are handled in accordance with the Smackdab Incident Response Plan (Security Policy §9) and the DPA (§5). Key requirements specific to data classification include: **Notification Timeline:** Client notification without undue delay and within forty-eight (48) hours of becoming aware of a confirmed Security Incident affecting Personal Data (DPA §5). **Classification-Based Response:** Incidents affecting PL-5 Restricted data receive the highest priority response with immediate escalation to the CISO and Legal team. Incidents affecting PL-4 Customer Data are treated as potential data breaches with mandatory customer notification assessment. **Notification Content:** Notifications include the nature of the incident, likely consequences, measures taken or proposed, and other information needed for Client's own notification obligations (DPA §5). **Post-Incident Review:** All incidents result in a post-incident review, root cause analysis, and updates to data classification and protection controls as needed.

---

11. TRAINING AND AWARENESS

All Smackdab Personnel receive training on this Policy as part of the broader security training program (Security Policy §4.4; Employee Data Handling Policy §11):

(a) Initial training on data classification and handling during onboarding;

(b) Annual refresher training on classification framework updates and data handling requirements;

(c) Role-specific training for Personnel with access to PL-3, PL-4, or PL-5 data;

(d) Simulated phishing exercises and security awareness campaigns; and

(e) Additional training when significant changes to this Policy or regulatory requirements occur. Training records including dates, content, and completion records are maintained by Human Resources in coordination with the Information Security Team.

12. POLICY REVIEW AND UPDATES

12.1. Review Schedule

This Policy is reviewed at least annually and updated as necessary to address changes in the threat landscape, technology, business practices, legal and regulatory requirements, results of audits and assessments, and CASA/OWASP ASVS framework updates.

12.2. Change Management

Material changes to this Policy require Security Committee review and recommendation, CISO approval, Executive Leadership approval for significant scope changes, and communication to all affected Personnel and, where applicable, Customers. The change notification process for Customers follows the procedures established in the Security Policy (§14.2), including at least 30 days' advance notice for material changes.

12.3. Version History

Version

Date

Author

Description

1.0

February 20, 2026

CISO

Initial release. Created to satisfy CASA / OWASP ASVS V1.8 and V8 requirements. Cross-referenced with DPA v2.0, Security Policy v2.0, and Employee Data Handling Policy v1.0.

13. CONTACT INFORMATION

For questions about this Policy, data classification decisions, or to report a concern: **Information Security Team:** security@smackdab.ai **Data Protection Officer:** dpo@smackdab.ai **Privacy Team:** privacy@smackdab.ai **Legal and Compliance:** legal@smackdab.ai **Mail:** Smackdab Inc. Attn: Information Security / Data Protection Officer 372 Live Oak Ln Marco Island, FL 34145 United States

This PDF is the formal downloadable version of EMPLOYEE DATA HANDLING POLICY.