



## LEGAL NOTICE

# Data Security Framework

A general description of Assivo's approach to information security, the limits of that description, and how security is addressed in client engagements.

---

|                      |                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------|
| Issued by            | <b>Assivo, Inc.</b>                                                                                            |
| Effective date       | <b>September 8, 2026</b>                                                                                       |
| Last updated         | <b>September 8, 2026</b>                                                                                       |
| Classification       | <b>Public</b>                                                                                                  |
| Official publication | <b><a href="https://assivo.com/legal/data-security-framework">assivo.com/legal/data-security-framework</a></b> |
| Outside counsel      | <b>Ian J. Block, Partner, Neal, Gerber &amp; Eisenberg LLP</b>                                                 |

# Contents

- Article I. Purpose, Status, and Interpretation
- Article II. Governance
- Article III. Reference Frameworks and Certifications
- Article IV. Areas of Control
- Article V. Client Systems and Shared Responsibility
- Article VI. Security Incidents
- Article VII. Disclaimer
- Article VIII. Contact
- Outside Counsel

# Article I. Purpose, Status, and Interpretation

## Section 1.01 Purpose

This Data Security Framework (this "Framework") gives a general description of the approach that Assivo, Inc. ("Assivo") takes to the security of information in its care across the operations of the Assivo Group, currently including Chicago, Mexico City, Mumbai, and Chennai.

## Section 1.02 Status of This Framework

This Framework is informational. It is not a contract, a warranty, a guarantee, a certification, an audit report, or a description of the controls applied in any particular engagement. It does not create any obligation on Assivo, any right in any client or other Person, or any duty of care. The security obligations that Assivo owes a client are exclusively those set out in the written agreement between Assivo and that client (the "Client Agreement"), and in the event of any inconsistency the Client Agreement governs.

## Section 1.03 No Reliance

This Framework is not intended to be, and must not be, relied on by any Person in deciding whether to engage Assivo, to provide information to Assivo, or for any other purpose. Any evaluation of Assivo's security should be conducted through Assivo's diligence process under a non-disclosure agreement, in which Assivo may make available its policies, assessment reports, and other evidence subject to confidentiality.

## Section 1.04 Point in Time

This Framework describes Assivo's general approach as of its effective date. Assivo's practices, tools, providers, and organization change over time, and Assivo may revise, replace, or withdraw this Framework at any time without notice. Assivo has no obligation to update this Framework to reflect changes in its practices. The version published at the address shown on the cover of this document is the authoritative version, and any other copy is superseded by it.

## Section 1.05 Definitions

- (a) "**Assivo Group**" means Assivo, Inc. together with its present and future parents, subsidiaries, affiliates, branches, and delivery entities in any jurisdiction, and their respective successors and assigns; and "**Assivo**" includes each member of the Assivo Group where the context permits.
- (b) "**Client Data**" means data that a client provides to Assivo, or that Assivo accesses in a client's systems, in the course of an engagement.
- (c) "**Person**" means any individual or entity.
- (d) "**Reference Frameworks**" means ISO/IEC 27001, the AICPA SOC 2 trust services criteria, and such other standards as Assivo may from time to time consult.

## Article II. Governance

Information security at Assivo is the responsibility of senior management, with day-to-day responsibility assigned to personnel in technology, operations, and legal roles. Assivo maintains written internal security policies, which are confidential, which it reviews periodically, and which its personnel are expected to follow. Internal policies may differ from this Framework and, where they do, this Framework does not describe them.

## Article III. Reference Frameworks and Certifications

### Section 3.01 Design Reference

Assivo designs its security program with reference to the Reference Frameworks and to the legal requirements that apply to the work it performs, which may include HIPAA, GDPR, and CCPA. Reference to a framework in this document is a description of design intent only.

### Section 3.02 No Certification Claim

Nothing in this Framework is a representation that Assivo is certified to, has been audited against, or complies in all respects with any Reference Framework or law. Any certification, attestation report, or audit result that Assivo holds is made available to clients and prospective clients only under a non-disclosure agreement and is subject to the scope, period, and qualifications stated in it.

## Article IV. Areas of Control

Assivo's program is organized around the following areas. The description of each area is general. The specific controls applied in any engagement depend on the data involved, the client's requirements, and the Client Agreement, and nothing below is a representation that any specific control is in place for any client.

- (a) **Classification and handling.** Information is categorized by sensitivity, and handling expectations are set accordingly.
- (b) **Access control.** Access to systems and data is intended to be granted on the basis of role and business need, authenticated, and periodically reviewed, and removed when no longer needed.
- (c) **Encryption.** Sensitive data is intended to be protected in transit and at rest using methods generally accepted in the industry.
- (d) **Endpoint and network protection.** Devices and networks used in Assivo's environment are intended to be protected, monitored, and maintained with current software.
- (e) **Physical security.** Assivo's delivery facilities are intended to be access-controlled.
- (f) **Personnel.** Personnel are screened to the extent permitted by local law, bound by written confidentiality obligations, and given security training.
- (g) **Third parties.** Vendors that access Assivo's or its clients' information are intended to be assessed and bound by contractual security and confidentiality terms.
- (h) **Logging and monitoring.** Activity on Assivo's systems is intended to be logged and monitored for security events.
- (i) **Incident response.** Assivo maintains internal procedures for responding to security incidents and for notifying affected clients as required by law and by the applicable Client Agreement.
- (j) **Continuity.** Assivo maintains backup and recovery arrangements for its core systems.
- (k) **Change and vulnerability management.** Assivo intends to manage changes to its environment and to address identified vulnerabilities on a risk-prioritized basis.

## Article V. Client Systems and Shared Responsibility

### Section 5.01 Work in Client Systems

In many engagements Assivo personnel perform work inside the client's own systems, under credentials that the client issues, controls, and can revoke. Where that is the case, the client's controls govern those systems and the data in them, and Assivo's controls apply to Assivo's own environment. Assivo does not assume responsibility for the security, configuration, or availability of any client system.

## **Section 5.02 Delivery Model**

Assivo determines in its sole discretion where, by whom, and through which members of the Assivo Group or which subcontractors its services are delivered, including through remote and international delivery, in order to optimize delivery, cost efficiency, and operational excellence, subject only to the express terms of the applicable written agreement. Any reference in this document to a location, facility, entity, or personnel is descriptive and is not a commitment as to where or by whom any service will be performed.

## **Section 5.03 Client Responsibilities**

Clients are responsible for their own security programs, for the systems they operate, for the instructions they give Assivo, for the classification of the data they entrust to Assivo, and for their own legal and regulatory obligations. Any allocation of responsibility beyond this Section is set out in the Client Agreement.

# **Article VI. Security Incidents**

## **Section 6.01 Client Notification**

Assivo notifies clients of security incidents affecting their Client Data as required by applicable law and by the applicable Client Agreement. This Framework does not establish any notification timeframe or content.

## **Section 6.02 Reporting a Concern**

Any Person who believes that an Assivo system or Assivo-held information may have been compromised may write to [security@assivo.com](mailto:security@assivo.com). Assivo reviews reports it receives and responds as it considers appropriate. Assivo does not operate a bug-bounty program and does not authorize testing of its systems by any Person.

# **Article VII. Disclaimer**

TO THE FULLEST EXTENT PERMITTED BY LAW, THIS FRAMEWORK IS PROVIDED FOR INFORMATION ONLY, WITHOUT WARRANTY OF ANY KIND, AND ASSIVO DISCLAIMS ALL LIABILITY ARISING FROM ANY PERSON'S USE OF OR RELIANCE ON IT. NO SECURITY PROGRAM CAN ELIMINATE ALL RISK, AND ASSIVO DOES NOT GUARANTEE THE SECURITY OF ANY INFORMATION.

## Article VIII. Contact

**Assivo, Inc.**

Attention: Information Security  
444 West Lake Street, Suite 1700, Chicago, Illinois 60606  
security@assivo.com

### Outside Counsel

Legal inquiries concerning this Data Security Framework may be directed to Assivo's outside counsel. This does not replace any notice address specified in this document.

**Ian J. Block**

Partner, Intellectual Property  
Neal, Gerber & Eisenberg LLP  
225 W. Randolph Street, Suite 2800, Chicago, Illinois 60606-1976  
Direct: (312) 269-2960 | iblock@nge.com

Contacting counsel through this document does not create an attorney-client relationship between Neal, Gerber & Eisenberg LLP and the person making contact. Counsel represents Assivo, Inc. only. Routine inquiries may also be sent to hello@assivo.com.

Assivo | 444 West Lake Street, Suite 1700, Chicago, IL 60606 | assivo.com