Filevine LOIS Evaluation Agreement

Last updated: July 17, 2026

Please read this Agreement carefully. By clicking "Submit," checking the box indicating your acceptance, or by accessing or using the Evaluation Services, you acknowledge that you have read and understood this Agreement and agree to be bound by its terms. If you do not agree, do not check the acceptance box and do not access or use the Evaluation Services.

This Filevine LOIS Evaluation Agreement (this "**Agreement**") is entered into between Filevine, Inc. ("**Filevine**") and the individual or entity ("**Evaluator**") accepting this Agreement and accessing Filevine's evaluation environment for its LOIS product (the "**Evaluation Services**"). If Evaluator is a natural person, Evaluator represents that Evaluator is at least eighteen (18) years of age or the age of legal majority in Evaluator's jurisdiction of residence. The individual accepting this Agreement on behalf of Evaluator, if Evaluator is an entity, represents that such individual has authority to bind such organization, and Evaluator represents that neither Evaluator nor any of its users is a competitor of Filevine or is accessing or using the Evaluation Services to assist a competitor of Filevine. Capitalized terms have the meanings given where first used in this Agreement.

1. Important Terms

1.1 **Incorporated Documents.** By accepting this Agreement or by accessing or using the Evaluation Services, Evaluator agrees to this Agreement together with the Filevine Data Protection Agreement (the "**DPA**") available at **https://www.filevine.com/data-protection-agreement/**, the Filevine Security Addendum (the "**Security Addendum**") attached hereto as Exhibit A, and the Filevine AI Acceptable Use Policy (the "**AI AUP**") attached hereto as Exhibit B, each incorporated by reference (collectively, the "**Agreement**").

1.2 **Updates.** Filevine may update this Agreement and the documents referenced in Section 1.1 from time to time, effective upon posting. Filevine shall not use this right to reduce its confidentiality or security commitments during Evaluator's evaluation without Evaluator's written consent.

1.3 **Order of Precedence.** If there is a conflict between this Agreement and (a) the DPA, the DPA controls as to data protection matters; (b) the Security Addendum, the Security Addendum controls as to security matters; and (c) the AI AUP, the AI AUP controls as to permitted and prohibited uses of AI-Enabled Features.

1.4 **AI Output.** The Evaluation Services include features powered by artificial intelligence ("**AI-Enabled Features**"), including features that rely on models provided by third-party AI providers. Output is AI-generated, may contain errors or omissions, and is provided for informational purposes only. Output is not legal advice, does not create an attorney-client relationship between Evaluator and Filevine, and must be independently reviewed by a qualified professional before use.

1.5 **Evaluation Purpose; Scope.** The Evaluation Services are made available solely so Evaluator can assess Filevine's LOIS product for a potential future purchase. The Evaluation Services consist of LOIS Console. Filevine case management offerings, custom workflows, enterprise integrations, and Filevine's full AI feature set are not included in the Evaluation Services and require a paid Sales Order. The Evaluation

Services may not include all support available under a paid Sales Order, including the availability and support commitments set forth in the Sales Order and Filevine Subscription Agreement.

2. Usage

2.1 **Grant.** Subject to this Agreement, Filevine grants Evaluator a limited, non-exclusive, non-transferable, revocable right to access and use the Evaluation Services solely for internal evaluation purposes during the Evaluation Period. Access credentials are specific to the individual to whom they are issued and may not be shared.

2.2 **Restrictions.** Evaluator will not, and will not permit any user to: (a) use the Evaluation Services in violation of applicable law or a third party's rights; (b) reverse engineer, decompile, or attempt to discover the source code, algorithms, or underlying models of the Evaluation Services; (c) circumvent or attempt to circumvent any security or access control of the Evaluation Services; (d) resell, sublicense, or make the Evaluation Services available to any third party; (e) use the Evaluation Services to build, or assist a third party in building, improving, or operating a competitive product or company; (f) use automated means to scrape or extract data or Output from the Evaluation Services other than such methods as are approved by Filevine; or (g) submit any protected health information, payment card data, social security numbers, government identification numbers, personally identifiable genetic or biometric data, or other highly sensitive data to the Evaluation Services.

3. Evaluation Data

3.1 **Ownership.** As between the parties, Evaluator owns all right, title, and interest in the data and content it submits to the Evaluation Services ("**Evaluation Data**"), including all information, analysis, or other content the Evaluation Services generate in response to Evaluation Data ("**Output**").

3.2 **License to Filevine.** Evaluator grants Filevine a non-exclusive, worldwide right to process Evaluation Data to provide the Evaluation Services and to prevent or address technical problems.

3.3 **Training; Third-Party AI Providers.** Filevine engages certain third-party AI providers to deliver AI-Enabled Features under written agreements prohibiting those providers from using Evaluation Data to train or improve their models, and under which those providers do not retain Evaluation Data beyond the applicable request, except for temporary retention solely for abuse-monitoring or trust-and-safety purposes.

3.4 **Aggregated and Anonymized Data.** Filevine may use Evaluation Data in de-identified, aggregated form ("**Anonymized Data**") to improve and enhance the Evaluation Services and for other development, diagnostic, and corrective purposes in connection with the Evaluation Services and other Filevine technologies and offerings, provided that Anonymized Data cannot reasonably be used to identify Evaluator or any individual, and Filevine does not attempt to re-identify Anonymized Data.

3.5 **Data Protection and Security.** The DPA and Security Addendum govern Filevine's processing and protection of Evaluation Data, including any Personal Information (as defined in the DPA), and are incorporated into this Agreement. For purposes of applying the DPA, Evaluator is deemed to be "Subscriber" and this Agreement, together with any Order Confirmation, is deemed to be a "Sales Order."

4. Fees

The Evaluation Services are provided to Evaluator at no cost during the Evaluation Period. Evaluator will use the Evaluation Services solely in accordance with Filevine's instructions for the evaluation. If Filevine reasonably believes Evaluator is not using the Evaluation Services in good faith for evaluation purposes, Filevine may immediately suspend or terminate Evaluator's access. Filevine may limit the resources, features, or usage volume available under this Agreement at any time.

5. Term and Termination

5.1 **Term.** This Agreement is effective upon Evaluator's acceptance of this Agreement or first access to the Evaluation Services, whichever is earlier, and continues for the period (the "**Evaluation Period**") stated in Filevine's written confirmation to Evaluator (an "**Order Confirmation**") or, if no Order Confirmation specifies a period, ninety (90) days from first access. Filevine may extend the Evaluation Period in its sole discretion upon Evaluator's written request.

5.2 **Termination.** Either party may terminate this Agreement at any time, for any reason, upon written notice to the other party.

5.3 **Effect of Termination.** Upon termination, Evaluator will stop using the Evaluation Services. Filevine's retention, return, and destruction of Evaluation Data following termination are governed by the Security Addendum.

5.4 **Conversion.** Upon execution of a Sales Order and related Subscription Agreement for the Services (as defined therein), this Agreement automatically terminates, and the Subscription Agreement (together with the applicable Sales Order) governs Evaluator's use of the Services going forward, without interruption in access.

5.5 **Survival.** Provisions that by their nature should survive termination will survive, including restrictions, confidentiality, ownership, warranty disclaimers, limitation of liability, dispute resolution, and other general terms.

6. Warranty; Disclaimer

6.1 **Evaluator Warranty.** Evaluator warrants that it has all rights necessary to submit Evaluation Data to the Evaluation Services and that its use of the Evaluation Services will comply with applicable law.

6.2 **Disclaimer. The Evaluation Services and all Output are provided "as is" and "as available," without warranty of any kind. Filevine disclaims all warranties, express or implied, including merchantability, fitness for a particular purpose, and non-infringement. Filevine does not warrant that the Evaluation Services will be uninterrupted, error-free, or secure, or that any Output will be accurate, complete, or reliable. Filevine is not a law firm and does not provide legal advice.**

7. Limitation of Liability

7.1 **Exclusion of Certain Damages. Neither party will be liable to the other for any indirect, incidental, special, exemplary, punitive, or consequential damages, including loss of income, profits, revenue, or business interruption, arising out of or in connection with this Agreement, whether or not advised of the possibility of such damages.**

7.2 **Liability Cap. Except for liability that cannot be limited by law, Filevine's total liability under this Agreement will not exceed $100,000.**

8. Confidentiality

Each party will protect the other's non-public information that is identified as confidential or that reasonably should be understood to be confidential given its nature or the circumstances of disclosure ("**Confidential Information**"), which includes Evaluation Data and Filevine's source code, algorithms, and underlying models, using at least the same degree of care it uses for its own confidential information of a similar nature (but not less than reasonable care), and will not use or disclose the other's Confidential Information except to perform its obligations under this Agreement or as required by law, with advance notice to the disclosing party where legally permitted. Each party may disclose the other's Confidential Information to employees, contractors, and advisors who need it for purposes consistent with this Agreement and who are bound to confidentiality obligations at least as protective as this Section. Unauthorized use or disclosure of Confidential Information may cause irreparable harm for which the disclosing party may seek injunctive relief without posting bond, in addition to other available remedies. This Section survives for three (3) years after termination, except that trade secrets remain protected for as long as they qualify for trade secret protection under applicable law.

9. General Terms

9.1 **Governing Law; Arbitration.** This Agreement is governed by the laws of the State of Utah, without regard to conflict-of-law rules. **EXCEPT FOR CLAIMS FOR INJUNCTIVE RELIEF AND PROCEEDINGS TO COMPEL ARBITRATION OR CONFIRM, VACATE, OR ENFORCE AN ARBITRAL AWARD, ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT WILL BE RESOLVED BY BINDING ARBITRATION IN SALT LAKE CITY, UTAH UNDER THE AAA COMMERCIAL ARBITRATION RULES BEFORE A SINGLE ARBITRATOR, WITH THE PREVAILING PARTY ENTITLED TO FEES AND COSTS**. The state courts located in Salt Lake County, Utah and the U.S. District Court for the District of Utah will have exclusive jurisdiction over claims and proceedings excluded from arbitration under this Section.

9.2 **Notice.** Notices to Filevine must be sent to legal@filevine.com. Notices to Evaluator may be sent to the email address associated with Evaluator's account.

9.3 **Severability.** If a provision is found unenforceable, the rest of this Agreement remains in effect.

9.4 **Export Control.** Evaluator represents that it is not located in an embargoed jurisdiction and is not on any U.S. government restricted-party list, and will comply with applicable export laws.

9.5 **Entire Agreement.** This Agreement, together with the DPA, Security Addendum, AI AUP, and any Order Confirmation, is the entire agreement between the parties regarding its subject matter and supersedes all prior discussions and agreements on that subject.

Filevine Security Addendum

This Security Addendum is part of the Agreement between Filevine, Inc. ("**Filevine**") and the customer identified in the applicable Sales Order ("**Subscriber**") and describes the security measures Filevine maintains to protect Subscriber's Data. Capitalized terms not defined in this Security Addendum have the meaning given in the Subscription Agreement or the DPA. To the extent of a conflict between this Security Addendum and the DPA regarding data protection matters, the DPA controls; to the extent of a conflict regarding technical or organizational security measures, this Security Addendum controls.

1. **Filevine Audits and Certifications**

   1.1. Filevine's information security program is assessed by independent third-party auditors on at least an annual basis through a SOC 2 Type II audit and an assessment against the ISO/IEC control frameworks. These frameworks currently include ISO 27001, ISO 27701, ISO 27017, ISO 27018 and ISO 42001, but may change from time to time. Filevine is aligned with NIST 800-53 Rev 5.* with respect to FedRAMP 20X Low & Moderate certifications for specific Filevine products.

   1.2. Where applicable to the Services purchased by Subscriber, Filevine's security program has also been assessed against the HIPAA Privacy & Security Rule and the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.9.5*.

   1.3. Filevine will make available a summary of its most recent audit report as described in Section 10 (Customer Audit Rights).

   1.4. If Filevine discontinues a certification or audit described in this Section 1, Filevine will endeavor to adopt an equivalent, industry-recognized framework in its place.

2. **Data Hosting Location**

   2.1. Subscriber's Data is stored and processed in data centers located in the United States, unless otherwise specified in the applicable Sales Order.

   2.2. Subscriber may request that its Data be stored in a specific geographic region. Filevine will use commercially reasonable efforts to accommodate such a request where supported by Filevine's underlying cloud infrastructure and consistent with applicable law.

3. **Encryption**

   3.1. Filevine encrypts Subscriber's Data at rest using AES-256* encryption, and in transit over public or untrusted networks using TLS 1.2*.

   3.2. Filevine utilizes an encryption key management system (KMS) and rotates encryption keys as needed, typically on an annual basis, and logically separates encryption key management systems from Subscriber's Data.

4. **System and Network Security**

4.1. Access to systems containing Subscriber's Data requires unique credentials issued consistent with the principle of least privilege, a secure connection, multi-factor authentication, and passwords meeting minimum length and complexity requirements.

4.2. Filevine personnel will not access Subscriber's Data except (a) to provide or support the Services, or (b) to comply with applicable law or a binding legal order.

4.3. Filevine personnel access Filevine's environment using company-managed devices employing encryption, endpoint detection and response tooling.

4.4. Filevine uses threat detection tooling to monitor for malicious code but has no obligation to monitor Subscriber's Data for malicious code.

4.5. Filevine engages an independent third party to conduct penetration testing of the Services at least annually and maintains an ongoing vulnerability management program, including a public bug bounty program. Summaries of penetration test results are available as described in Section 10 (Customer Audit Rights).

4.6. Filevine monitors public vulnerability databases and uses commercially reasonable efforts to remediate identified vulnerabilities within a risk-appropriate timeframe based on severity and exploitability.

4.7. Filevine conducts annual web application security assessments, including testing for vulnerability classes identified by the Open Web Application Security Project (OWASP Top 10), such as cross-site scripting, cross-site request forgery, and injection vulnerabilities.

5. **Administrative and Personnel Controls**

5.1. Filevine personnel receive security awareness training at onboarding and at least annually thereafter, covering individual security and privacy responsibilities, Filevine's information security policies, phishing and social engineering awareness, and device and credential hygiene.

5.2. Filevine trains software developers on secure development practices at least annually, including prevention of common vulnerability classes such as injection, cross-site scripting, and authentication or authorization bypass.

5.3. Filevine personnel sign confidentiality agreements and are required to report suspected security incidents.

5.4. To the extent permitted by applicable law, Filevine performs background screening — including identity verification, right-to-work verification, and a criminal history check — for personnel with access to Subscriber's Data. For applicable staff, additional screening, such as that required by CJIS, FedRAMP, or government agency obligations, is performed.

5.5. Access for departing personnel is removed from systems containing Subscriber's Data within one (1) business day and from all other systems within three (3) business days. Filevine reviews personnel access privileges at least quarterly.

5.6. Filevine monitors external threat intelligence sources, such as FBI or CISA advisories, and prioritizes remediation of critical and high-severity vulnerabilities consistent with Section 4.6.

6. **Vendor and Sub-processor Security**

6.1. Before engaging a material Sub-processor to process Subscriber's Data, Filevine assesses the Sub-processor's security practices and requires by written agreement that the Sub-processor maintain security measures designed to be no less protective than those described in this Security Addendum, to the extent applicable to the services it provides.

6.2. Filevine maintains a current list of Sub-processors at **https://www.filevine.com/subprocessors/.**

6.3. Filevine will exercise commercially reasonable care in the selection and oversight of its Sub-processors' acts and omissions only to the extent Filevine would be responsible if it performed the applicable services directly.

7. **Physical Data Center Controls**

7.1. The Services are hosted on infrastructure provided by leading cloud infrastructure providers, independently audited under SOC 2 Type II and ISO 27001 (or an equivalent framework), with controls that include: controlled facility ingress; visitor identification and sign-in; access-controlled server areas subject to periodic review; monitoring, alarm, and video surveillance coverage; fire detection and suppression systems; backup power and redundancy; and environmental controls.

7.2. Filevine does not host or store Subscriber's Data at its corporate offices.

8. **Security Incident Notification and Response**

8.1. If Filevine confirms a breach of security leading to the destruction, loss, alteration, or unauthorized disclosure of, or access to, Subscriber's Data (a "**Security Breach**"), Filevine will notify Subscriber without undue delay, at the contact identified in the applicable Sales Order.

8.2. Filevine will promptly investigate, contain, and remediate the Security Breach, and will endeavor to preserve logs relevant to the Security Breach for at least one (1) year.

8.3. Filevine will provide Subscriber with timely information regarding the nature and consequences of the Security Breach, the status of its investigation, and a point of contact for further information, and will share information about remediation measures once the investigation concludes. Subscriber acknowledges that because Filevine personnel may have limited visibility into the content of Subscriber's Data, Filevine's ability to describe the specific Data affected may be limited.

8.4. Communications made in connection with a Security Breach will not be construed as an admission of fault or liability by Filevine.

8.5. Except where the Security Breach arises from Subscriber's instructions, negligence, or breach of the Agreement, Filevine will bear its own reasonable costs of investigating and remediating the Security Breach.

9. **Audit Logging**

9.1. Filevine maintains audit logs reasonably sufficient to monitor, investigate, and report unauthorized or inappropriate system activity, with actions of individual users traceable to those users.

9.2. Audit logs are retained for at least one (1) year and are encrypted and protected against unauthorized modification or deletion.

10. **Customer Audit Rights**

10.1. Upon written request, and at no additional cost to Subscriber, Filevine will provide Subscriber (or its appropriately qualified third-party representative, the "**Auditor**") with Filevine's most recent SOC 2 Type II report. Filevine may provide evidence of Filevine's ISO 27001 status, a summary of Filevine's most recent penetration test, and/or a data flow diagram for the applicable Filevine Service. Any third-party Auditor must execute a confidentiality agreement with Filevine before receiving this documentation, and Filevine may reasonably object to an Auditor it believes is not suitably qualified, in which case Subscriber will designate an alternative Auditor.

10.2. Subscriber may submit a security questionnaire (not to exceed fifty (50) questions in any twelve (12) month period) or a request for updated security documentation, and Filevine will respond within six (6) weeks at no cost to Subscriber.

10.3. If the documentation described in Section 10.1 is unavailable or Subscriber reasonably requires further verification, Filevine will permit Subscriber (or its Auditor) to audit Filevine's compliance with this Security Addendum upon at least thirty (30) days' written notice, subject to reasonable scheduling and confidentiality protections.

11. **Subscriber Responsibilities**

11.1. Subscriber is responsible for ensuring it is authorized to submit its Data to the Services and that its use complies with applicable law.

11.2. Subscriber is responsible for managing and securing its own means of accessing the Services, including Logon Credentials, private API keys, personal access tokens (PATs), and shared or guest links. Credentials may not be shared, and Subscriber must promptly report any suspected unauthorized access and confirmed breach events.

11.3. Subscriber is responsible for keeping its own IT systems — including the browser used to access the Services — up to date and appropriately patched, and for enabling available security features such as multi-factor authentication for its Authorized Users.

11.3.1. Shared Responsibility Model:

Filevine Responsibilities

- AWS infrastructure security
- Encryption in transit and at rest
- Application-level access controls
- Centralized monitoring and incident response
- Platform availability and backups

Subscriber Responsibilities

- Identity provider security
- User provisioning and deprovisioning
- MFA enforcement
- Tenant configuration
- Tenant activity monitoring
- Endpoint and network security
- Regulatory compliance and data governance

11.4. Filevine disclaims liability for Security Breaches or other security incidents to the extent arising from Subscriber's failure to satisfy its obligations under this Section 11.

12. **Business Continuity and Disaster Recovery**

12.1. Filevine maintains business continuity and disaster recovery plans addressing the key personnel, systems, and processes needed to restore the Services following a significant disruption. These plans are reviewed and tested regularly.

13. **Data Retention and Destruction**

13.1. Following termination or expiration of the Subscription Agreement, Filevine is not obligated to retain Subscriber's Data for more than thirty (30) days, subject to Subscriber's timely election under the Subscription Agreement to have such Data destroyed or returned. Upon written request, Filevine will provide written certification of deletion or destruction of Subscriber's Data.

** Where a version, revision, standard, or protocol in this Security Addendum is marked with an asterisk, Filevine may satisfy the applicable commitment using the stated item or any successor or higher version, or a substantially equivalent or more protective standard, that Filevine adopts from time to time.*

Filevine AI Acceptable Use Policy

This Filevine AI Acceptable Use Policy (this "**AI AUP**") is part of the Subscription Agreement between Filevine, Inc. ("**Filevine**") and the customer identified in the applicable Sales Order ("**Subscriber**") and governs use of AI-Enabled Features (features of the Filevine Services that use artificial intelligence, including LOIS). Capitalized terms not defined in this AI AUP have the meaning given in the Subscription Agreement.

Permitted Uses

Subject to this AI AUP and the Subscription Agreement, Subscriber and its Authorized Users may use AI-Enabled Features for Subscriber's lawful internal business purposes, including, but not limited to, drafting, reviewing, and summarizing documents and correspondence, legal research and analysis, and case or matter assessment, in each case subject to Section 3 (AI-Powered Services and Output) of the Subscription Agreement, including the human-review responsibilities described there.

Prohibited Uses

Subscriber will not, and will not permit any Authorized User or third party to, use AI-Enabled Features to: (a) generate or disseminate content that is unlawful, fraudulent, or defamatory, or that infringes a third party's intellectual property or privacy rights; (b) engage in unlawful discrimination against individuals on the basis of a legally protected characteristic; (c) create deepfakes, synthetic impersonations of real individuals, or fabricated evidence intended to deceive; (d) reverse-engineer, decompile, or attempt to derive the source code, model weights, training data, or architecture of any AI model used in the AI-Enabled Features; (e) circumvent or attempt to circumvent any safety filter, usage limit, or access control of the AI-Enabled Features; (f) develop, train, or benchmark a product or service that competes with the Filevine Services; or (g) use automated means to scrape or extract Output from the AI-Enabled Features outside ordinary use.

High-Risk and Regulated Decision-Making

Subscriber will not use AI-Enabled Features to make, assist, or serve as a substantial factor in making a decision that produces legal or similarly significant effects on an individual (including decisions regarding an individual's access to employment, housing, credit, insurance, healthcare, or government benefits) without meaningful review by a qualified professional. Where Subscriber's use of AI-Enabled Features is subject to state or federal law governing automated decision-making (including the Colorado AI Act), Subscriber is responsible for complying with all applicable requirements, including any required disclosures and human-review processes.

Sensitive Data

Subscriber should exercise particular care before submitting protected health information, personal information of minors, privileged or court-sealed material, or other legally or contractually sensitive data to AI-Enabled Features, and is responsible for confirming that doing so is permitted under applicable law and Subscriber's own confidentiality obligations.

Questions about this AI AUP may be directed to legal@filevine.com.