Terms of Service

AssureOne provides the Services to you in accordance with and subject to the following Terms of Service ("Terms"). These Terms set forth the terms and conditions under which you may use the Service in accordance with the Agreement and govern your access to and use of all software, mobile apps, websites and related services provided to you by AssureOne (collectively, the "Services"). The Services are owned and provided by AssureOne Technologies LLC (the "Company", "we," "our," or "us").

Please read these Terms carefully before you begin using the Services. By using the Services or signing up for an Account, you accept and agree to be bound by and comply with these Terms, the Privacy Policy and other applicable policies and terms. If you do not agree with the Terms, you may not access or use the Services.

1. Definitions

The following definitions apply to these Terms:

"Account" means the account created or maintained to access and use the Services.

"AI Credits" means usage units applied to certain AI Features and used to measure or calculate consumption of those features.

"AI Features" means artificial intelligence, machine-learning, generative AI, and automated functionality made available through the Services.

"AssureOne" or "Platform" means the proprietary cloud-based software platform owned and operated by the Company under the AssureOne brand, including its applications, portals, APIs, modules, workflows, AI Features, integrations, and related functionality.

"AssureOne Technology" means the Services and all related Intellectual Property Rights, including software, designs, interfaces, databases, APIs, models, algorithms, workflows, templates, documentation, know-how, trade secrets, trademarks, and other technology owned or licensed by the Company, excluding Customer Data and Customer-owned materials.

“Authorized User” means any employee, contractor, consultant, representative, client, or other individual whom the Customer authorizes to access or use the Services through the Customer's Account. An Authorized User does not become a Customer merely by accessing or using the Services.

“Commercial Terms” means the pricing, billing, usage, renewal, and other commercial terms applicable to the Customer, whether set out in an order form, pricing page, purchase screen, subscription confirmation, or other document affirmatively accepted by the Customer's authorized Account owner or billing administrator.

“Confidential Information” means any non-public information disclosed by or on behalf of one party (the “Disclosing Party”) to the other party (the “Receiving Party”) that is marked or identified as confidential or that, considering its nature and the circumstances of disclosure, should reasonably be understood to be confidential. Customer Data is the Customer's Confidential Information. The Services, non-public technical and security information concerning the Platform, pricing, product plans, and AssureOne Technology are the Company's Confidential Information.

“Customer” means an individual acting in a professional or business capacity, or a legal entity, that is identified as the Account owner and accepts these Terms, whether in connection with a Trial Period, Subscription, or other use of the Services.

“Customer Data” means all data, documents, records, information, and content uploaded, submitted, imported, transmitted, or otherwise provided to the Services by or on behalf of you or your Authorized Users, including third-party data that you are authorized to provide.

“Data Processing Addendum” or “DPA” means a standalone data processing addendum entered into by, or otherwise applicable to, the Company and the Customer in connection with the Services, or the data processing terms contained in a Signed Addendum such as Engagement Letter, that are expressly intended to govern the Processing of Personal Data.

“Fees” means all subscription fees, AI Credit charges, Usage-Based Charges, overage charges, and other amounts payable under these Terms, the applicable Commercial Terms, or a Signed Addendum.

“Intellectual Property Rights” means all patent, copyright, trademark, trade-secret, database, design, know-how, proprietary, and other intellectual property or similar rights, whether registered or unregistered.

“Output” means any content, text, data, analysis, or other material generated by or through an AI Feature in response to a prompt, instruction, or automated process.

“Personal Data” means any information relating to an identified or identifiable natural person, household, or other protected individual, and includes personal data, personal information, and similar terms as defined under applicable data protection law.

“Privacy Policy” means the Company's privacy policy made available through the Services or at the Company's website, as updated from time to time.

“Process,” “Processed,” or “Processing” means any operation performed on Personal Data, including collecting, accessing, recording, organizing, storing, altering, retrieving, using, disclosing, transmitting, restricting, deleting, or otherwise handling Personal Data.

“Security Incident” means any confirmed unauthorized access to, acquisition, use, alteration, disclosure, loss, or destruction of Customer Data in the Company's possession or control. A Security Incident does not include unsuccessful attempts or activities that do not compromise Customer Data, including unsuccessful login attempts, port scans, denial-of-service attacks, or similar events.

“Signed Addendum” means an engagement letter, statement of work, amendment, or other written document signed by both the Company and the Customer that expressly supplements or modifies these Terms. A Signed Addendum may include data processing terms that constitute an applicable DPA.

“Services” means all products, modules, features, functionality, websites, applications, portals, APIs, AI Features, integrations, support, and related services made available by the Company through AssureOne.

“Subscription” means any paid plan made available for continued access to the Services, including any recurring, usage-based, or combined pricing arrangement applicable to the Account.

“Third-Party Services” means any third-party software, application, website, platform, API, AI provider, payment processor, integration, or other service that connects with, supports, or is accessible through the Services.

“Trial Period” means a limited period during which an eligible Customer may access specified Services without a recurring platform subscription fee, subject to these Terms, applicable Commercial Terms, and any Fees or Usage-Based Charges.

“Agreement” means these Terms, the applicable Commercial Terms and any DPA or Signed Addendum that expressly incorporates or supplements these Terms.

“Usage-Based Charges” means Fees calculated by reference to actual use of the Services, including AI Credit consumption, processing volume, features used, integrations, users, or other usage metrics disclosed in the applicable Commercial Terms.

“you” or “your” means the Customer and, where the context concerns access or use by an individual, the applicable Authorized User; however, obligations allocated to the Customer remain the Customer's responsibility.

“Usage Data” means technical, operational and statistical information generated through the use of the Services, excluding Customer Data, prompts, uploaded files and Output.

2. Eligibility and Accounts

Eligibility

The Services are intended for lawful professional and business use. You must be legally capable of entering into a binding contract and, if acting for an organization, authorized to accept these Terms on its behalf. You may not use the Services if applicable law prohibits access; applicable trade sanctions prevent access, or we previously suspended or terminated your access for misuse unless we give written permission to return.

You must provide accurate, current, and complete registration, contact, and billing information, keep that information updated, and reasonably cooperate with verification of your identity, organization, domain, professional status, payment method, or authority to act.

Accounts and Authorized Users

You may create an Account and authorize employees, partners, contractors, consultants, clients, or other Authorized Users to access features you make available. You are responsible for Account configuration, administrator permissions, connected services, payment methods, AI usage, workflows, invitations, and client-facing access.

You must protect login credentials, authentication codes, API keys, and tokens; limit access to persons who need it; promptly remove access when a role or relationship ends; and notify us at legal@assureone.ai if you suspect unauthorized access or credential compromise.

We may rely on instructions and actions taken through an authenticated Account as authorized by the Customer and may temporarily restrict access when we reasonably suspect fraud, compromised credentials, or a security threat.

You are responsible for the acts and omissions of your Authorized Users in connection with the Services and for ensuring that they comply with these Terms and your applicable security, confidentiality, privacy, and professional obligations. The Company is not responsible for unauthorized access, disclosure, loss, misuse, or a Security Incident caused by the negligence, misconduct, credential compromise, improper access permissions, or other acts or omissions of you, your personnel, contractors, or Authorized Users, except to the extent directly caused by Company's breach of its own obligations under these Terms.

3. Services

The Company makes the Services available through the AssureOne platform as described in the applicable Commercial Terms or Signed Addendum.

Descriptions on our website or in marketing materials, demos, roadmaps, or other general communications are provided for general information only and do not modify, expand, or create obligations under these Terms. Features, availability, limits, beta status, and service levels may vary by plan, Account, geography, release stage, or technical readiness and may change, subject to any notice or commitment expressly stated in the applicable Commercial Terms or Signed Addendum.

4. Subscription, Trial, and Fees

Commercial Terms and Fees

The applicable Commercial Terms, or Signed Addendum will identify the Services, Fees, billing frequency, usage allowances, Trial Period, renewal and cancellation terms, and any Usage-Based Charges. Website or purchase-screen terms apply only if affirmatively accepted by the Customer's authorized Account owner or billing administrator.

You must pay all Fees when due under the applicable Commercial Terms or Signed Addendum. Rates, units, minimums, included allowances, overages, and billing methods will be disclosed before the relevant paid use begins. Taxes, duties, and similar governmental charges may be added where required by law.

Trial, Renewal, and Cancellation

A Trial Period provides limited evaluation access and may exclude features, Third-Party Services, support levels, usage capacity, or other functionality. Unless the applicable Commercial Terms or a Signed Addendum states otherwise, we may modify or end a Trial Period at any time, and a Trial Period does not include free or unlimited AI processing.

Continued access may require a Subscription, Usage-Based Charges, or both. Renewal, cancellation, post-cancellation access, treatment of prepaid Fees or unused AI Credits, outstanding Usage-Based Charges, and any refund rights are governed solely by the applicable Commercial Terms or Signed Addendum.

Billing and Payment Processing

Fees are generally stated in U.S. dollars and exclude taxes unless stated otherwise. You must maintain a valid payment method and accurate billing information. If you believe a charge is incorrect, contact legal@assureone.ai within seven (7) days after the charge or invoice date and provide sufficient information for us to investigate. Undisputed overdue amounts may accrue interest at the lesser of one percent (1%) per month or the maximum rate permitted by law, and we may restrict paid functionality after reasonable notice.

We may use Stripe or another Third-Party Service to process payments. The payment provider may collect and process payment cards or bank information under its own terms. We do not store full card numbers, card verification values, or online-banking credentials on our systems.

For platform billing, we receive only payment and transaction information reasonably necessary to process charges, manage refunds, address disputes, and maintain records.

If you use client-payment functionality, the applicable Third-Party Service acts as payment processor, and you remain responsible for the underlying invoice, service, tax, refund, dispute, authorization, and client relationship. Any provider fees will be governed by the provider's terms or disclosed before the transaction.

5. Customer Data

Ownership and License

Customer Data may include business information, personal information, accounting records, financial data, tax documents, audit materials, workpapers, client communications, engagement details, contact data, workflow information, files, images, forms, signatures, prompts, and other content uploaded, submitted, created, imported, synchronized, transmitted, or generated through the Services.

You retain ownership of Customer Data. You give us a limited, non-exclusive, worldwide license to host, transmit, display, organize, analyze, transform, back up, and otherwise process Customer Data only as reasonably necessary to provide, secure, support and maintain the Services; follow your instructions; prevent fraud and abuse; comply with law; and enforce these Terms.

You are responsible for Customer Data and for making sure you have the rights, permissions, notices, consents, and lawful basis needed to place it in the Services. Before adding information belonging to a client, employee, contractor, vendor, taxpayer, meeting participant, or other person, you must determine and obtain any permission or consent required by law, contract, professional duties, or your own privacy notices.

Processing and Verification

The Services may process, organize, analyze, extract, classify, transform, or otherwise handle Customer Data as described in the applicable Commercial Terms or a Signed Addendum. Automated processing may be inaccurate, incomplete, or unavailable.

You must verify processed or transformed information against source materials before relying on it and remain responsible for retention, archival, deletion, independent backups, lawful-use requirements, and professional or regulatory obligations.

Storage, Retention, Backups, and Content Management

We may apply storage or Processing limits under the applicable Commercial Terms. If usage exceeds applicable limits or materially affects platform stability, security, cost, or other users, we may require an upgrade, apply reasonable throttling or restrictions, or charge applicable Fees after reasonable notice, except where immediate action is necessary for security, abuse prevention, or system protection.

We generally retain Customer Data for the duration of your use of the Services. Following termination or expiration of your Account, we may provide a thirty (30) day period during which you may retrieve or export available Customer Data, after which we may delete or render such data inaccessible, subject to applicable legal, regulatory, professional, backup, or record-retention requirements.

We maintain commercially reasonable backup, business-continuity, and disaster-recovery measures designed to support restoration following material disruption. Backups are maintained primarily for disaster recovery and service continuity, are not an individual file-restoration or archival service and may not recover the most recent changes. You must maintain independent copies of critical records, filed documents, final work product, and materials required by professional or legal obligations.

We may remove, disable access to, quarantine, or suspend processing of any content that we reasonably believe is unlawful, infringing, malicious, harmful, unauthorized, or in violation of these Terms or our Acceptable Use requirements as per Section 11. Where reasonably practicable, we will provide notice before or promptly after taking such action, unless notice creates a security risk, interfere with an investigation, violate law, or impair our ability to prevent misuse of the Services.

Audit trails and electronic records

The Services may create logs and audit trails showing account access, timestamps, IP addresses, document uploads and downloads, versions, edits, approvals, signatures, workflow transitions,

user invitations, integration events, AI requests, messages, billing activity, and security actions. We use these records to operate and secure the Services, support users, investigate misuse, maintain continuity, and comply with law.

Audit trails are generated from system activity and may not capture events that occur outside AssureOne, events blocked by a third party, or actions performed before logging is enabled. You should review audit information relevant to your work and maintain any independent records required by your procedures or professional standards. To the extent permitted by law, electronic logs and records may be used as evidence of activity conducted through an authenticated account.

6. Artificial Intelligence

How AI Features work

AssureOne uses artificial intelligence technologies to assist with document classification, data extraction, summarization, drafting, search, workflow suggestions, reconciliation support, gap detection, note-taking, and other tasks. AI Features may use models and infrastructure supplied by us or by third-party providers, including OpenAI and Microsoft-hosted AI services where enabled. Your use of AI Features through AssureOne is governed by these Terms, the Privacy Policy, any applicable DPA, and any applicable Signed Addendum. If you independently access or contract with a third-party AI provider outside the Services, that independent use is governed by the provider's applicable terms and privacy policy.

No training on Customer Data

We do not use Customer Data, or de-identified or aggregated content derived from Customer Data to train or fine-tune any artificial intelligence or machine-learning model, whether public, private, internal, or third-party. We contractually require third-party AI providers used for production features to process Customer Data only as necessary to provide the requested service and not to use Customer Data to train or improve their general-purpose models.

We will not use identifiable Customer Data to advertise to the Customer or its clients or to develop products unrelated to the Services. We may use aggregated or de-identified technical, operational, and service-usage information that does not contain Customer Data, identify you, your

organization, your clients, or any individual to measure performance, improve workflows, detect errors, develop features, understand usage, operate and secure the Services, and describe general platform performance. We will not use such information to train or fine-tune an artificial intelligence or machine-learning model or represent it as identifiable Customer Data.

You must verify every Output

AI and automated software produce probabilistic results. Output may be inaccurate, incomplete, outdated, duplicated, inconsistent, biased, misleading, or fabricated. It may misunderstand a document, omit a material fact, use an incorrect date or amount, apply an unsuitable accounting or tax treatment, or fail to reflect current law, guidance, or professional standards.

You must ensure that all material Output generated or used by you or your Authorized Users is independently reviewed and verified before using it in a ledger, workpaper, financial statement, tax return, audit file, client communication, engagement letter, filing, report, invoice, recommendation, or business decision. A qualified person must compare Output with source records and apply professional judgment. Alerts, reminders, anomaly indicators, and workflow status are convenience tools and must not be your only control for deadlines, filing obligations, approvals, or quality review.

You control whether to accept, edit, reject, publish, file, send, sign, or act on Output. We do not review or approve your professional work and do not guarantee that Output is suitable for your purpose. You must not tell a client or regulator that the Company has certified, endorsed, or approved your work merely because it was created or processed through AssureOne.

Your prompts and responsible use

You are responsible for prompts, instructions, source materials, and decisions made using AI Features. Do not use AI Features to generate unlawful, deceptive, discriminatory, infringing, malicious, or fraudulent content; to make a high-impact decision without appropriate human review; to impersonate a person; or to conceal the use of AI where disclosure is required.

Do not submit information to an AI Feature unless you are authorized to process it in that way. This is especially important for tax return information, government identifiers, financial credentials, regulated information, confidential client materials, and recorded or transcribed

communications. You must obtain any required consent before using AI to process another person's information.

Ownership of AI Output

As between you and the Company, and to the extent permitted by applicable law, you own the Output generated specifically for you from Customer Data. The Company does not claim ownership of such Output and assigns to you any rights it may have in it. You may use Output for any lawful purpose, subject to these Terms.

The Company retains all rights in the Services and its models; Company-provided prompts, workflows, templates, algorithms, system instructions, software and underlying technology. No rights in these materials transfer to you merely because they are used to generate Output. Because artificial intelligence may generate similar or identical Output for different users, Output may not be unique or protectable under intellectual-property law, and the Company does not guarantee that Output is free from third-party claims.

7. Integrations and Communications

Third-Party Services and Data Migration

The Services may connect with Third-Party Services to support data import, synchronization, communications, document management, payments, and related workflows. Available integrations may be described on our website or in the Services and may change as providers, APIs, and product priorities evolve.

When you connect a Third-Party Service, you authorize us to access, retrieve, receive, transmit, and synchronize the categories of information permitted through the applicable authorization screen and reasonably necessary for the relevant feature. You are responsible for connecting only Accounts you are authorized to use, reviewing permissions, maintaining valid credentials, and disconnecting access when no longer required.

Where data migration is included in the applicable Commercial Terms or a Signed Addendum, we may assist with importing or mapping available data from existing systems. You remain responsible for ensuring that data supplied for migration is complete, accurate, lawfully obtained,

authorized for transfer, and independently backed up before migration. Migration may be affected by data quality, file formats, third-party APIs, system configurations, compatibility, interruptions, or limitations outside our control.

Third-Party Services currently offered, planned, or referenced for the platform may include Google Workspace, including Gmail, Google Calendar, and Google Drive; Microsoft 365, including Outlook, Calendar, OneDrive, and SharePoint; accounting systems such as QuickBooks Online and Xero; and other tax, bookkeeping, audit, document management, communication, identity verification, and workflow tools made available through the platform.

Your independent use of Third-Party Services is governed by the applicable provider terms and privacy policies, which you should review before connecting the service. We recommend reviewing the applicable terms and conditions, privacy policies, and related policies of each third-party Service mentioned above.

Third-party terms and policies do not amend, limit, or reduce the Company's obligations under these Terms, any applicable DPA, or Signed Addendum, or under applicable law.

Information obtained through a Third-Party Service may be delayed, incomplete, duplicated, reformatted, or affected by the provider's settings or systems. You must verify imported or synchronized information before relying on it. A Third-Party Service may become unavailable if the provider modifies or discontinues its API, permissions, pricing, security requirements, services, or applicable terms.

Service communications

We may send transactional and service-related communications by email, SMS, telephone, or in-platform notification. These may include authentication codes, Account alerts, security notices, document requests, e-signature requests, workflow reminders, billing notices, AI Credit alerts, integration failures, product changes, support messages, and legally required notices.

Transactional communications are part of the Services and are not marketing. You may be unable to opt out of communications necessary to operate or secure your Account. Marketing communications will include an available opt-out method where required by law. Message and data rates may apply to SMS. You must ensure that phone numbers and email addresses you

provide are accurate and that you have permission to use them for the communications you initiate through the Services.

If you enable recording, transcription, or AI note-taking, you are responsible for telling participants and obtaining any consent required by call-recording, wiretap, employment, professional, or privacy law. The Services must not be used for emergency communications.

8. Privacy, Security, and Data Protection

How privacy responsibilities are divided

Our Privacy Policy explains how we collect, use, disclose, retain, and protect Personal Data in connection with the Services. When you place Personal Data in Customer Data, you generally decide why and how that information is used, and we process it to provide the Services and follow your lawful instructions. Depending on the law, you may be the controller or business and we may be the processor or service provider.

You are responsible for determining which privacy, professional, tax, employment, records, communication, and industry rules apply to your use. You must provide required notices, obtain consent, honor applicable rights, and avoid placing information in the Services when you lack authority to process it. We will reasonably assist with verified privacy requests relating to Customer Data where required and technically feasible.

Applicable privacy laws and international Processing

Depending on the relevant persons and locations, use of the Services may be subject to the EU General Data Protection Regulation ("GDPR"), applicable U.S. state privacy laws, and other privacy and data-protection laws.

Customer Data and Personal Data may be Processed in the United States and other countries where the Company, its affiliates, or sub processors operate, including jurisdictions that may not provide an equivalent level of protection and in which information may be accessible to governmental authorities. Where required by applicable law, the parties will use an appropriate transfer mechanism, including standard contractual clauses or another lawful safeguard, and will enter into or otherwise be subject to applicable data processing addendum (the "DPA").

Sub processors

We use sub processors and service providers to operate the Services. These may include Microsoft Azure and Amazon Web Services (AWS) for cloud hosting and infrastructure; OpenAI and other approved AI providers for AI Features; Stripe for payment processing; Twilio for SMS services; and other providers supporting email, authentication, monitoring, support, analytics, security, and the Third-Party Services you choose.

Sub processors may process Customer Data only to the extent reasonably necessary to provide their services to us and are subject to appropriate confidentiality, privacy, and security obligations. We may maintain a current list of material sub processors on our website or make it available on request. We may change sub processors as the Services evolve and will provide notice where the DPA or applicable law requires it.

For further information regarding the services and data-processing practices of our sub processors, kindly visit their website for terms and conditions, privacy policy and other applicable terms governing the use of their services.

Security

We use commercially reasonable administrative, technical, organizational, and physical safeguards designed to protect Customer Data. Depending on the feature and environment, safeguards may include, as appropriate, encryption in transit and at rest, access controls, role-based permissions, multi-factor authentication, secure development practices, logging, monitoring, vulnerability management, malware controls, backups, incident response, and disaster recovery.

No online platform is completely secure. You are responsible for security on your devices, networks, email accounts, connected systems, and user accounts. Use strong unique passwords, enable multi-factor authentication where available, keep software updated, restrict administrator access, train users, review permissions, and promptly remove departing personnel.

If we become aware of a Security Incident affecting Customer Data under our control, we will notify affected account administrators without undue delay and as required by applicable law or the applicable DPA. Notice may include available information about the nature of the incident and reasonable steps you can take. You must promptly notify us of a suspected incident involving your

account. We may provide information in phases as it becomes available, and our notice will not be construed as an admission of fault or liability.

Professional and regulatory compliance

AssureOne is designed to support your workflows and does not guarantee compliance with laws, regulations, or professional standards applicable to your activities. You remain responsible for meeting all applicable legal, regulatory, licensing, professional, confidentiality, record-retention, tax, accounting, audit, industry, sanctions, export-control, anti-bribery, and similar obligations, and for obtaining any required consents or authorizations before processing regulated information through the Services. Do not upload or process information subject to special legal requirements, including protected health information, unless the Company has expressly approved such use and any required Agreement is in place.

9. Confidentiality

Confidential Information does not include information that the Receiving Party can demonstrate: (a) is or becomes publicly available without breach of these Terms; (b) was lawfully known to the Receiving Party without confidentiality restriction before disclosure; (c) is received lawfully from a third party without breach of any confidentiality obligation; or (d) is independently developed without use of or reference to the Disclosing Party's Confidential Information.

The Receiving Party will: (i) use Confidential Information only to perform its obligations or exercise its rights under these Terms, the applicable Commercial Terms or a Singed Addendum; (ii) protect Confidential Information using at least reasonable care and no less than the care it uses to protect its own confidential information of a similar nature; and (iii) disclose Confidential Information only to its employees, affiliates, contractors, professional advisers, and service providers who have a legitimate need to know and are bound by confidentiality obligations at least as protective as those set out in these Terms. The Receiving Party remains responsible for any breach of this Section by persons to whom it discloses Confidential Information.

If the Receiving Party is legally compelled to disclose Confidential Information, it may do so only to the extent legally required and, where legally permitted, will provide the Disclosing Party with prompt notice and reasonable assistance in seeking confidential treatment or a protective order.

Upon termination of the applicable Services or upon written request, the Receiving Party will, within thirty (30) days, return or delete the Disclosing Party's Confidential Information that is no longer reasonably necessary to perform its obligations or exercise its rights under these Terms, the applicable Commercial Terms, applicable DPA, or a Signed Addendum. Customer Data will be retained, made available for retrieval, returned, and deleted exclusively in accordance with Section 5 and any applicable DPA. The Receiving Party may retain Confidential Information to the extent required by applicable law, professional obligations, applicable DPA, or ordinary backup and archival processes. Any retained Confidential Information will remain protected under this Section and will not be used for any other purpose.

These confidentiality obligations will continue for five (5) years after disclosure or termination of the Services, whichever is later. Obligations relating to trade secrets will continue for so long as the information remains a trade secret under applicable law. Obligations relating to Customer Data and Personal Data will continue for as long as such information remains in the Receiving Party's possession or control.

Each party acknowledges that unauthorized use or disclosure of Confidential Information may cause irreparable harm for which monetary damages may be inadequate. Accordingly, the Disclosing Party may seek appropriate injunctive or equitable relief, in addition to any other available remedies.

10. Intellectual Property

Our technology

The Company and its licensors exclusively own all right, title, and interest in and to the AssureOne Technology. Except for the limited rights expressly granted in these Terms or a Signed Addendum, no right, title, or interest in AssureOne Technology is transferred or assigned to you, and all rights not expressly granted are reserved by the Company and its licensors.

While your access remains authorized and you comply with these Terms and applicable payment obligations, we grant you a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to access and use the Services solely for your organization's lawful internal and client-service activities through the functionality we make available. This license does not extend to the

source code, underlying architecture, or any AssureOne Technology outside the functionality made available to you, and no licenses are granted by implication, estoppel, or otherwise. Any improvement, enhancement, configuration, or derivative work that we create to or from the Services whether or not prompted by your feedback, use, or data remains AssureOne Technology and is owned exclusively by the Company. For clarity, AssureOne Technology does not include Customer Data, other Confidential Information of the Customer, or Customer-owned materials merely because they are processed through the Services. To the extent permitted by applicable law, you waive, and agree not to assert, any moral or similar rights in any feedback or suggestions you provide to us.

Trademarks and Open Source

AssureOne, AssureOne Technologies LLC, related product and service names, logos, and branding are trademarks and trade dress of the Company or its licensors. You may not use them without our prior written permission, except to accurately identify the Services you use, and any resulting goodwill inures solely to the Company's benefit. You may not remove, obscure, or alter any proprietary notice appearing on or in the Services.

The Services may include open-source components governed by their own licenses. Those licenses control for the applicable component and do not grant rights to proprietary parts of the Services.

Feedback and De-identified Information

If you provide ideas, suggestions, or feedback about the Services, you grant us a worldwide, perpetual, irrevocable, royalty-free, transferable, and sublicensable right to use and incorporate that feedback without restriction or compensation, provided we do not publicly identify you as the source without permission.

Subject to Section 6, we may create aggregated or de-identified statistics and insights solely from Usage Data and use them to operate, secure, benchmark and improve the Services and describe general platform performance.

We will take reasonable measures to ensure that de-identified information cannot be associated with an identified or identifiable individual, will not attempt to re-identify it, and will contractually require any recipient to comply with equivalent restrictions.

This right does not permit us to derive such information from the content of Customer Data, prompts, instructions, uploaded files or Output, or to use Usage Data to train or fine-tune any artificial-intelligence or machine-learning model. If you have any concerns regarding content available through the Services, including a concern that it infringes your copyright, please email us at legal@assureone.ai.

11. Acceptable Use

You must not and must ensure that your Authorized Users do not use the Services in a way that harms people, violates law, interferes with the platform, compromises data, or misuses our technology. In particular, you must not:

- access or attempt to access an account, system, data set, API, or feature without authorization;
- share credentials, bypass usage limits, defeat security controls, probe vulnerabilities without written permission, or interfere with availability or performance;
- upload malware, ransomware, malicious code, unlawful content, infringing material, or information you are not authorized to process;
- use bots, scrapers, or automated extraction except through supported APIs or export tools;
- reverse engineer, decompile, disassemble, decrypt, decode, or otherwise attempt to discover or reconstruct the source code, underlying algorithms, models, non-public APIs, technical architecture, or other proprietary components of the Services, or use non-public aspects of the Services to develop a competing product or service, except to the extent such restrictions are prohibited by applicable law;
- use the Services for fraud, impersonation, deceptive practices, spam, harassment, unlawful discrimination, sanctions evasion, or infringement;
- use AI Features to generate malicious code, facilitate illegal conduct, make unsupported decisions, mislead clients about human review, or process regulated information without required authorization;

- use the Services for competitive benchmarking or to train, develop, or improve a competing model or service without written permission;
- consume unreasonable storage, computing, messaging, or API resources in a way that threatens fair use, security, or platform stability; or
- resell, lease, sublicense, or provide the Services as a standalone service bureau unless we expressly authorize it.

We may investigate suspected violations, preserve relevant records, remove content, limit functionality, suspend access, or cooperate with authorities where reasonably necessary. We will consider context, severity, risk, and whether a violation can be corrected before taking action, except where immediate action is needed to protect people, data, systems, or legal compliance.

12. Suspension and Termination

Suspension

We may temporarily limit or suspend access if we reasonably believe your use, or the use of any Authorized User, creates a security risk, violates these Terms, exposes us or others to liability, is fraudulent, materially disrupts the Services, violates law, or involves overdue undisputed charges. Where practical, we will provide notice and an opportunity to correct the issue. We may act immediately where delay could increase harm.

Ending use of the Services

You may stop using the Services at any time. Ending a Trial Period or Account does not cancel Fees already incurred, including consumed AI Credits and completed Usage-Based Charges. Instructions for closing an Account or requesting export or deletion may be available through the Services or support.

We may terminate your access if you or any of your Authorized Users materially or repeatedly violate these Terms, fail to cure a remediable breach after notice, do not pay undisputed charges, misuse the Services, create an unacceptable security or legal risk, or if we discontinue the Services. We may also end a trial or free feature at any time.

When access ends, your permission to use the Services ends. Provisions that by their nature should continue including ownership, confidentiality, data retention, disclaimers, liability limits, indemnification, dispute resolution, and payment obligations survive.

13. Disclaimers, Limitation of Liability, and Indemnification

No professional advice

The Company provides technology through AssureOne. The Company does not provide accounting, tax, audit, assurance, legal, investment, financial, or other professional advice. Information and Output available through the Services are not a substitute for advice from a qualified professional who understands the relevant facts and current law. You are solely responsible for professional conclusions, filings, representations, reports, and services delivered to your clients.

Limited mutual warranty

Each party represents and warrants that it has the legal power and authority to enter into these Terms and that doing so will not violate any Agreement to which it is a party. The Company additionally warrants that it will perform the Services in a professional and workmanlike manner consistent with generally accepted industry standards. Your sole and exclusive remedy, and Company's entire liability, for breach of the warranty in the preceding sentence is that the Company will use commercially reasonable efforts to correct the non-conforming Services or, if we are unable to do so within a reasonable time, refund the fees you paid for the affected Services for the affected period.

Services otherwise provided as available

EXCEPT FOR THE EXPRESS WARRANTIES IN THE “LIMITED MUTUAL WARRANTY” SUBSECTION ABOVE, AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE SERVICES, DOCUMENTATION, OUTPUT, BETA OR PREVIEW FUNCTIONALITY, THIRD-PARTY SERVICES, AND CONTENT SUPPLIED BY THIRD PARTIES ARE PROVIDED “AS IS” AND “AS AVAILABLE,” WITHOUT WARRANTY OF ANY KIND. WE DISCLAIM ALL OTHER EXPRESS, IMPLIED, AND STATUTORY WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR

PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, SECURITY, AVAILABILITY, AND ERROR-FREE OPERATION.

WE DO NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, THAT OUTPUT WILL BE ACCURATE OR COMPLETE, THAT DEFECTS WILL BE CORRECTED, THAT DATA WILL NEVER BE LOST, OR THAT THE SERVICES WILL MEET EVERY PROFESSIONAL, REGULATORY, OR BUSINESS REQUIREMENT. SOME JURISDICTIONS DO NOT ALLOW CERTAIN DISCLAIMERS, SO PART OF THIS SECTION MAY NOT APPLY TO YOU.

Limitation of liability

TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE COMPANY AND ITS AFFILIATES, OFFICERS, EMPLOYEES, CONTRACTORS, LICENSORS, AND SERVICE PROVIDERS WILL NOT BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES; LOSS OF PROFITS, REVENUE, BUSINESS, GOODWILL, OR DATA; BUSINESS INTERRUPTION; COST OF SUBSTITUTE SERVICES; OR LOSSES ARISING FROM YOUR CLIENT RELATIONSHIPS, PROFESSIONAL WORK, AI OUTPUT, INTEGRATIONS, OR THIRD-PARTY SERVICES, EVEN IF ADVISED THAT SUCH DAMAGES ARE POSSIBLE.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, OUR TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THE SERVICES OR THESE TERMS WILL NOT EXCEED THE GREATER OF (A) THE TOTAL FEES YOU PAID TO THE COMPANY FOR THE SERVICES DURING THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM, OR (B) ONE HUNDRED U.S. DOLLARS (US $100). THESE LIMITATIONS APPLY REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, AND EVEN IF A LIMITED REMEDY FAILS OF ITS ESSENTIAL PURPOSE. YOU MUST BRING ANY CLAIM RELATING TO THESE TERMS, THE SERVICES, PRIVACY POLICY, APPLICABLE COMMERCIAL TERMS OR ANY SIGNED ADDENDUM WITHIN ONE (1) YEAR AFTER THE CLAIM ARISES, OR IT IS PERMANENTLY BARRED.

The pricing and availability of the Services reflect this allocation of risk.

Indemnification obligations

To the fullest extent permitted by law, you will defend, indemnify, and hold harmless the Company, its affiliates, and their respective officers, directors, members, employees, contractors, agents, successors, and assigns from and against any third-party claim, action, investigation, proceeding, demand, loss, liability, damage, judgment, penalty, fine, cost, or reasonable attorneys' fees arising out of or relating to:

(a) your Customer Data or your collection, use, disclosure, processing, transfer, storage, or submission of such data;

(b) your professional services, advice, work product, filings, returns, reports, communications, or relationship with your clients or other third parties;

(c) your violation of any applicable law, privacy or data protection requirement, cybersecurity obligation, professional standard, licensing requirement, or duty owed to a third party;

(d) your failure to obtain or maintain any required consent, authorization, privacy notice, permission, or lawful basis for the collection, processing, disclosure, transfer, or use of Personal Data or other regulated information;

(e) any unauthorized access, security incident, data breach, malware, credential compromise, or loss or disclosure of information resulting from your systems, devices, personnel, Authorized Users, access permissions, Account credentials, security practices, or third-party services connected by you;

(f) your failure to implement reasonable security measures, safeguard account credentials, appropriately manage Authorized User access, or promptly notify us of known or suspected unauthorized access to your Account;

(g) your or any Authorized User's misuse of the Services or violation of any intellectual property, privacy, confidentiality, data protection, or other third-party right; or

(h) your material breach of these Terms or any material breach of these Terms by an Authorized User.

This indemnity will not apply to the extent a claim is finally determined by a court of competent jurisdiction or in a final arbitral award to have resulted directly from the Company's fraud, willful misconduct, gross negligence, or material breach of its own obligations under these Terms. This indemnification obligation is in addition to, and not in lieu of, any other right or remedy available to us and it is not subject to the cap in the "Limitation of liability" subsection above.

Indemnification procedure

The indemnified party will (i) provide the indemnifying party with prompt written notice of the claim, provided that a delay in notice will relieve the indemnifying party of its obligations only to the extent the delay materially prejudices its defense; (ii) allow the indemnifying party to control the defense and settlement of the claim with counsel of its choosing; and (iii) provide reasonable cooperation, at the indemnifying party's expense, in connection with the defense and settlement. The indemnifying party will not enter into any settlement that admits fault by, or imposes any non-monetary obligation on, the indemnified party without the indemnified party's prior written consent, not to be unreasonably withheld.

14. Dispute Resolution and Governing Law

Informal resolution

Before commencing arbitration or filing a claim that is permitted to proceed in court, the parties will attempt in good faith to resolve the dispute informally. If you are raising the dispute, you must send written notice describing the issue and requested resolution to the legal-notice contact specified in Section 17. If the Company is raising the dispute, the Company will send notice to the contact information associated with your Account. Authorized representatives will have thirty (30) days after receipt of the notice to discuss resolution before either party commences a proceeding, except that either party may seek urgent injunctive or equitable relief at any time.

Governing law

Except to the extent a Signed Addendum expressly provides otherwise for its subject matter, these Terms and any dispute, claim, or controversy arising out of or relating to these Terms, the Services, applicable DPA or a Signed Addendum, including their formation, interpretation, breach, termination, or validity, are governed by and construed in accordance with the laws of the State of

Delaware, without regard to its conflict-of-laws principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

Arbitration

Except as provided in the "Exceptions; Class Action and Jury Trial Waiver" subsection, and unless a Signed Addendum provides otherwise, any dispute arising out of or relating to these Terms, the Services, applicable DPA, or a Signed Addendum including its formation, interpretation, breach, termination, or validity that remains unresolved after informal resolution will be determined by final and binding individual arbitration administered by the American Arbitration Association ("AAA") under its then-current Commercial Arbitration Rules. The Federal Arbitration Act governs this arbitration provision.

The arbitrator may grant any individual remedy available in court, subject to these Terms and any applicable Signed Addendum. The award will be final and may be enforced in any court of competent jurisdiction. The arbitration will remain confidential except as necessary to conduct or enforce it, comply with law, or make required disclosures. Fees and costs will be allocated under the AAA Rules, and attorneys' fees may be awarded only as permitted by these Terms, applicable Signed Addendum, or law.

Exceptions; class action and jury trial waiver

Notwithstanding the arbitration requirement, either party may bring an eligible claim in small-claims court and may seek urgent injunctive or other equitable relief in any court of competent jurisdiction to protect Intellectual Property Rights, Confidential Information, data, or security pending arbitration. To the maximum extent permitted by law, each party may bring claims only in its individual capacity and not as a plaintiff or class member in any class, collective, consolidated, mass, or representative action or arbitration. The arbitrator may not consolidate claims or award relief for persons or entities other than the individual parties. For any claim permitted to proceed in court, each party waives trial by jury. If a waiver in this paragraph is unenforceable for a particular claim, that portion will be severed and the remainder of this Section will continue to apply.

15. Changes to These Terms

We may update these Terms as the Services, business model, technology, law, and risk environment change. If we make a material change, we will provide reasonable advance notice by email, in-platform notice, or posting an updated version with a new 'Updated On' date, unless immediate change is needed for security, legal compliance, or to prevent harm.

Your continued use of the Services after updated Terms take effect means you accept the changes. If you do not agree, you must stop using the affected Services before the new Terms take effect. Changes do not retroactively alter charges already incurred or claims that arose before the applicable change takes effect unless law requires otherwise.

16. General Provisions

- You may not assign these Terms without our written consent, except in connection with a merger, reorganization, or sale of substantially all assets where the successor agrees to these Terms.
- Nothing in these Terms restricts either party from expressing lawful and truthful opinions or making disclosures protected by applicable law. However, neither party shall knowingly publish or communicate false statements of fact concerning the other party, misuse the other party's Confidential Information, or make statements in violation of applicable law.
- Neither party is liable for delay or failure caused by events beyond reasonable control, including natural disasters, war, civil unrest, labor disputes, utility or internet failures, cyberattacks, provider outages, epidemics, governmental actions, or changes in law, except that this does not excuse payment obligations already incurred.
- If a provision is unenforceable, it will be modified to the minimum extent necessary and the remainder will continue. Failure to enforce a provision is not a waiver. Headings are for convenience.
- The parties are independent contractors; these Terms do not create a partnership, agency, employment, fiduciary, franchise, or joint-venture relationship.
- Neither party has authority to bind or incur obligations on behalf of the other. Your Subscription to or use of the Services does not create any ownership, membership, partnership, agency, or other proprietary interest in the Company or AssureOne.

- Notices from us may be delivered by email, in-platform notification, or posting through the Services. Legal notices to the Company must be sent to legal@assureone.ai and are effective when received. Electronic records and signatures satisfy writing and signature requirements to the extent permitted by the ESIGN Act, UETA, and other applicable law.

17. Contact Us

Questions about these Terms or the Services may be sent to us using the following contact:

Mailing address: 16192 Coastal Highway, Lewes, Delaware 19958.

Email: legal@assureone.ai