Master Services Agreement

Version 1.0 | Effective Date of this Version: November 18, 2026

Published at https://www.databitinc.com/legal/msa. Prior versions are archived at https://www.databitinc.com/legal/msa/archive.

How this MSA works
This Master Services Agreement ("MSA") contains the standard legal terms under which Databit, Inc. provides services. It does not by itself obligate either party to buy or provide anything. It applies when Client signs an Engagement Document (such as Managed Services Terms, Cloud & Licensing Resale Terms, a Statement of Work or a quote) that refers to this MSA by version number. Please read Sections 6 (Suspension), 7 (Term and Termination), 11 (Limitation of Liability) and 14 (Disputes, including the jury trial waiver) carefully.

1. Definitions

Capitalized terms have the meanings below or where they are first defined in quotation marks.

1.1 **"Agreement"** means this MSA together with each Engagement Document that incorporates it. Each Engagement Document, together with this MSA, forms a separate contract.

1.2 **"Authorized Contact"** means an individual designated by Client in an Engagement Document, the client portal or in writing to request services, approve charges or receive notices on Client's behalf. Client is bound by the requests and approvals of its Authorized Contacts.

1.3 **"Business Day"** means Monday through Friday, excluding the Observed Holidays listed in Schedule 1.

1.4 **"Client"** means the entity identified as the client in an Engagement Document.

1.5 **"Client Data"** means data, files, email and other content that Client or its users store or process using the Services or the Client Environment, including Personal Data, but excluding Service Data.

1.6 **"Client Environment"** means the hardware, software, networks, cloud tenants, accounts and other IT assets owned, leased, licensed or used by Client, wherever located.

1.7 **"Databit"** means Databit, Inc., a New Jersey corporation, with its principal office at 200 Route 17, Mahwah, New Jersey 07430.

1.8 **"Engagement Document"** means a document signed (including electronically) or accepted by both parties that describes specific Services and Fees and incorporates this MSA, including Managed Services Terms, Cloud & Licensing Resale Terms, Statements of Work, quotes and order forms.

1.9 **"Fees"** means all amounts payable by Client under the Agreement, including recurring, usage-based, one-time, time-and-materials, pass-through and termination-related amounts.

1.10 **"Notice Period"** means the period between delivery of a termination notice and the effective date of termination.

1.11 **"Personal Data"** means information that identifies or is reasonably linkable to an individual and that is protected by applicable privacy or data-security law.

1.12 **"Security Incident"** means a confirmed unauthorized access to, or acquisition, disclosure, encryption or loss of, Client Data.

1.13 **"Service Data"** means logs, telemetry, configuration data, tickets and similar data generated by Databit's tools or in the course of providing the Services.

1.14 **"Services"** means the services, products and deliverables Databit provides under an Engagement Document, including Third-Party Services resold or arranged by Databit.

1.15 **"Third-Party Provider"** means any person other than Databit and Client that supplies software, cloud services, hardware, connectivity, security tools, data-center or hosting capacity, help-desk, network or security operations support, distribution or other goods or services used to deliver the Services, including manufacturers, publishers, distributors and subcontractors.

1.16 **"Third-Party Services"** means goods, software, subscriptions, licenses and services supplied by a Third-Party Provider, whether resold by Databit, bundled into a Databit Service, or purchased by Client directly.

2. Structure of the Agreement; Updates to this MSA

2.1 **Incorporation.** Each Engagement Document that refers to this MSA incorporates it by reference, as identified by its version number and effective date. By signing or accepting an Engagement Document, Client confirms that it has had the opportunity to review this MSA.

2.2 **Order of Precedence.** If documents conflict, the following order controls: (a) a written amendment signed by both parties; (b) the Engagement Document, but only where it expressly states that it overrides a specific Section of this MSA; (c) this MSA, including Schedule 1; and (d) quotes, invoices and other ordering documents. Terms in Client purchase orders, vendor portals or similar documents do not apply, even if accepted or signed by Databit, unless expressly agreed in a signed amendment.

2.3 **Version Control.** Databit may publish updated versions of this MSA at the address above. Each version will show a version number and effective date, and Databit will keep prior versions available at the archive address above. The version identified in an Engagement Document applies to that Engagement Document until replaced under Section 2.4.

2.4 **Effect of Updates on Existing Engagements.** The version of this MSA identified in an Engagement Document governs that Engagement Document until replaced under this Section. (a) Signed adoption. If Client signs or accepts an Engagement Document, quote or renewal that identifies a later version, that later version governs all of Client's Engagement Documents from the date of signature or acceptance. (b) Notice. Otherwise, Databit will give Client at least thirty (30) days' written notice of an updated version, by email to Client's primary and billing contacts and by posting the updated version and a summary of the changes at the address above, and the updated version applies to Client's existing Engagement Documents from the effective date stated in the notice. (c) Objection. If an update materially and adversely affects Client, Client may object by written notice delivered before the updated version's effective date. Databit will then, at its option, either (i) continue to apply the prior version to Client's Engagement Documents until the end of the then-current term, or (ii) permit Client to terminate the affected Engagement Documents on sixty (60) days' written notice without the Notice Period payment under Section 7.4, in which case Client remains responsible for Fees for Services performed through the termination date and for non-cancellable Third-Party Services commitments. (d) Changes that do not adversely affect Client, or that are required by law, regulation or a Third-Party Provider, take effect on the date stated in the notice and are not subject to objection. No update changes the Fees stated in an Engagement Document except as permitted by Section 5.6.

2.5 **No Other Changes.** Except as stated in Section 2.4 and Section 5.6, the Agreement may be amended only by a written document signed by both parties.

3. Services

3.1 **Scope.** Databit will provide the Services described in each Engagement Document. Anything not expressly included in an Engagement Document is out of scope.

3.2 **Out-of-Scope Work and Projects.** Databit may provide out-of-scope services, projects and after-hours work on request at the rates in the applicable Engagement Document or, if none, Databit's then-current rates. Projects will be quoted separately. Approval thresholds for out-of-scope charges are set out in Schedule 1.

3.3 **Service Standards.** Managed services are delivered under the service standards in Schedule 1. Response and resolution times are targets, not guarantees, and no service credits or refunds apply to missed targets unless an Engagement Document expressly provides for them.

3.4 **Use of Third-Party Providers.** Databit uses Third-Party Providers to deliver Services and may add, replace or remove any Third-Party Provider, product or tool at any time without Client's consent. A change of provider does not by itself reduce the scope of Services described in the applicable Engagement Document. Third-Party Providers that store or process Client Personal Data on Databit's behalf ("Data Sub-processors") will be bound by written contract to data-protection obligations at least as protective as Section 8, and Databit will maintain a current list of Data Sub-processors at www.databitinc.com/legal/subprocessors; updating that list is notice of the change. Any additional notice or objection rights for Data Sub-processors apply only if set out in a data-protection addendum, business

associate agreement or Engagement Document signed by Databit. Databit remains responsible for the performance of its own personnel and of subcontractors acting under Databit's direction, but not for the products, platforms, outages, security or acts or omissions of other Third-Party Providers.

3.5 **Third-Party Services.** Third-Party Services are provided under, and Client's use of them is subject to, the applicable Third-Party Provider's terms, policies and service levels ("Third-Party Terms"), including the Microsoft Customer Agreement where applicable. Client will comply with Third-Party Terms and authorizes Databit to accept, or attest to Client's acceptance of, Third-Party Terms on Client's behalf where the Third-Party Provider permits. Databit does not control and is not responsible for the availability, performance, security, data handling, pricing, changes or discontinuation of Third-Party Services. Databit's only obligation for a Third-Party Service failure is to use commercially reasonable efforts to report and pursue the issue with the Third-Party Provider and to pass through any warranty or remedy the provider makes available.

3.6 **Tools and Agents.** Databit may install remote monitoring and management, security, backup and similar software agents in the Client Environment. These tools remain the property of Databit or its licensors, are licensed to Client only for use with the Services, and will be removed or disabled when the Services end. Client will not remove, disable or interfere with them during the term.

3.7 **AI-Assisted Tools.** Databit may use automation and AI-assisted tools to deliver the Services, subject to its confidentiality and data-protection obligations under the Agreement. Databit will not knowingly permit Client Confidential Information to be used to train artificial intelligence models made generally available to third parties.

3.8 **Recommendations and Declined Services.** Databit may recommend changes, upgrades or security controls (for example, multi-factor authentication, endpoint protection, backups or replacement of unsupported systems). If Client declines, defers or fails to implement a recommendation, Client accepts the associated risk, and Databit is not responsible for losses that the recommendation was reasonably designed to prevent. Databit may ask Client to confirm a declined recommendation in writing.

3.9 **Hardware and Procurement.** Title to and risk of loss for hardware and other goods purchased through Databit pass to Client on delivery. Manufacturer warranties are passed through to Client and are Client's sole remedy for defective goods. Returns are subject to the manufacturer's or distributor's policies, including restocking fees. Special orders are non-cancellable once placed.

4. Client Responsibilities

4.1 **Cooperation and Access.** Client will provide timely access to the Client Environment, premises, information, documentation and decision-makers that Databit reasonably needs, designate Authorized Contacts, and keep its contact information current. Databit is not responsible for delays or failures caused by Client's failure to do so.

4.2 **Minimum Standards.** Client will maintain the Client Environment in line with the minimum standards in Schedule 1. Systems that do not meet them may be supported on a best-efforts, out-of-scope basis or excluded from coverage.

4.3 **Licensing.** Client is responsible for obtaining and maintaining valid licenses for all software and services in the Client Environment, other than licenses Databit expressly agrees to supply.

4.4 **Changes by Others.** Client will not allow anyone other than Databit to change covered systems without notifying Databit. Work required because of changes made by Client or third parties is out of scope.

4.5 **Client's Legal Obligations.** Client remains responsible for its own compliance with laws and regulations that apply to its business and data, including privacy, data-breach, record-retention, industry and employment laws. Databit does not provide legal or compliance advice.

4.6 **Data Retention and Backups.** Client is responsible for deciding what data must be backed up and for how long. Databit has no backup obligation unless an Engagement Document includes backup services. Where it does, Databit will perform the backup services described, but does not guarantee that every file or system can be restored.

4.7 **Insurance.** Each party will maintain insurance appropriate to its business. Client is encouraged to maintain cyber liability insurance. Databit will provide a certificate of its insurance on request.

4.8 **Safety and Conduct.** Client will provide a safe workplace and inform Databit of site safety rules. Databit may withdraw personnel from, or decline to visit, a site that Databit reasonably considers unsafe. Each party will treat the other's personnel professionally and courteously.

5. Fees, Invoicing and Payment

5.1 **Invoicing.** Unless an Engagement Document states otherwise, recurring Fees are invoiced monthly in advance on the first day of each month and are due no later than the fifth (5th) day of that month. Usage-based Fees, time-and-materials work, overages and other non-recurring Fees are invoiced monthly in arrears and are due within thirty (30) days of the invoice date. One-time onboarding and project deposits are due on signature unless stated otherwise.

5.2 **Payment Method.** Databit may require payment by ACH or automatic card payment. Any credit card surcharge will not exceed Databit's actual cost of processing and will be disclosed as required by law.

5.3 **Late Payment.** Past-due amounts bear a late charge of one and one-half percent (1.5%) per month, or the maximum rate permitted by law if lower, from the due date until paid. Client will also pay a returned-payment fee of $35 for each dishonored payment and Databit's reasonable costs of collection, including attorneys' fees and collection-agency fees.

5.4 **Invoice Disputes.** Client must notify Databit in writing of any good-faith invoice dispute, with reasonable detail, within thirty (30) days of the invoice date, and must pay the undisputed portion when due. The parties will work in good faith to resolve the dispute. Invoices not disputed within that period are deemed accepted.

5.5 **Taxes.** Fees exclude sales, use, excise and similar taxes, which Client will pay (other than taxes on Databit's income). If Client claims an exemption, it must provide a valid exemption certificate.

5.6 **Price Adjustments.** Databit may (a) pass through increases in Third-Party Provider prices, taxes or regulatory charges on written notice, effective when the increase applies to Databit; and (b) increase other recurring Fees once in any twelve (12) month period, on at least thirty (30) days' written notice, by up to the percentage stated in the Engagement Document or, if none is stated, five percent (5%).

5.7 **No Set-Off.** Client will pay all Fees without set-off, counterclaim, deduction or withholding, except for taxes Client is legally required to withhold.

6. Suspension of Services

6.1 **Suspension for Non-Payment.** If any undisputed amount owed under any Engagement Document is more than fifteen (15) days past due, Databit may suspend all or part of the Services under any Engagement Document until Client's account is paid in full, after giving Client a final written notice, by email to Client's billing and primary contacts, at least ten (10) days before suspension that identifies the past-due amount and states that suspension may result in loss of access to systems and permanent loss of Client Data.

6.2 **Third-Party Services.** Without limiting Section 6.1, if Client does not pay any amount owed for Third-Party Services when due, Databit may, after the notice required by Section 6.1, (a) suspend, disable, downgrade or stop renewing the affected Third-Party Services, and (b) stop paying the applicable Third-Party Providers for those Third-Party Services, in each case until Client's account is current. Third-Party Providers may suspend, de-provision or delete accounts, tenants, subscriptions, backups and stored data after non-payment under their own policies and retention periods, which Databit does not control.

6.3 **Loss of Access and Data. CLIENT ACKNOWLEDGES THAT SUSPENSION OF SERVICES OR THIRD-PARTY SERVICES UNDER THIS SECTION 6, AND ANY RESULTING ACTION BY A THIRD-PARTY PROVIDER, MAY CAUSE LOSS OF ACCESS TO SYSTEMS, EMAIL, APPLICATIONS AND DATA AND THE PERMANENT LOSS OR DELETION OF CLIENT DATA, INCLUDING BACKUPS. EXCEPT TO THE EXTENT CAUSED BY DATABIT'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, DATABIT IS NOT LIABLE FOR ANY LOSS OF ACCESS, LOSS OF DATA, BUSINESS INTERRUPTION OR OTHER DAMAGES RESULTING FROM A SUSPENSION MADE IN ACCORDANCE WITH THIS SECTION 6.**

6.4 **Data During Suspension.** During any suspension, Databit will not itself delete Client Data from Databit-controlled systems. On Client's written request and prepayment at Databit's then-current rates, Databit will give Client a reasonable opportunity to export Client Data held in Databit-controlled systems. Client acknowledges that it is solely

responsible for keeping its account current and for maintaining its own copies of Client Data it considers critical, and that a suspension made in accordance with this Section 6 is not a breach of the Agreement by Databit.

6.5 **Suspension to Protect Systems.** Databit may immediately suspend any Service, account or connection, without prior notice, if reasonably necessary to respond to an active security threat, to prevent harm to the Client Environment, Databit's systems or third parties, or to comply with law or a Third-Party Provider's requirements. Databit will notify Client as soon as practicable and restore the Service when the reason for suspension ends.

6.6 **Fees and Reinstatement.** Fees continue to accrue during any suspension caused by Client. Databit will restore suspended Services promptly after Client pays all past-due amounts and any reactivation charges imposed by Third-Party Providers. Databit cannot guarantee that data deleted by a Third-Party Provider can be recovered.

6.7 **Client Indemnity for Suspension.** Client will defend, indemnify and hold harmless Databit from any third-party claim arising from a suspension made in accordance with this Section 6, except to the extent caused by Databit's gross negligence or willful misconduct.

7. Term, Renewal and Termination

7.1 **Term of this MSA.** This MSA applies for as long as any Engagement Document that incorporates it remains in effect.

7.2 **Term and Automatic Renewal of Engagements.** Unless the Engagement Document states otherwise, each Engagement Document has an initial term of twelve (12) months starting on its service start date ("Initial Term") and then renews automatically for successive twelve (12) month terms (each a "Renewal Term"), without limit, unless terminated as permitted by the Agreement.

7.3 **Renewal Reminders.** Where applicable law requires advance notice of an automatic renewal, including New York General Obligations Law § 5-903 for Clients located in New York or receiving Services at New York locations, Databit will send Client a written reminder of the automatic renewal, in the form and within the time the law requires (for § 5-903, by certified mail or personal delivery at least fifteen (15) and not more than thirty (30) days before the last day on which Client may give notice to avoid renewal; where the Notice Period is one hundred eighty (180) days, that day is 180 days before the end of the then-current term). If Databit does not send a reminder required by applicable law, the Engagement Document will continue on a month-to-month basis, terminable by either party on thirty (30) days' written notice, until the next anniversary of its service start date for which Databit has sent the reminder, and will then renew as provided in Section 7.2.

7.4 **Termination by Client for Convenience.** Client may terminate an Engagement Document at any time by giving at least one hundred eighty (180) days' written notice. The parties agree that this Notice Period reflects the time reasonably required to transition the Services to Client or a new provider, to wind down Third-Party Services commitments and reconcile Fees billed in arrears, and Databit's commitment of personnel, tools and capacity to Client. During the Notice Period: (a) Databit will continue to provide and keep available the Services; (b) recurring Fees for Databit's managed services will continue to be invoiced, and are payable as they come due, through the end of the Notice Period; (c) Third-Party License Fees and other Fees billed in arrears will be invoiced based on actual quantities and usage through the date the applicable Third-Party Services are cancelled, transferred or expire, together with any non-cancellable commitments; and (d) Migration Services are provided as described in Section 7.8.

7.5 **Termination by Databit.** Databit may terminate any Engagement Document (a) without cause, on thirty (30) days' written notice, or (b) immediately on written notice for Cause. "Cause" means: (i) any amount is more than thirty (30) days past due; (ii) Client materially breaches the Agreement and the breach cannot be cured or is not cured within ten (10) days after written notice; (iii) Client becomes insolvent, makes an assignment for the benefit of creditors, or is the subject of a bankruptcy or receivership proceeding; (iv) Client or its personnel engage in abusive, threatening, unsafe or unlawful conduct toward Databit personnel; (v) Client uses the Services in violation of law or Third-Party Terms; or (vi) Client refuses to remedy a condition in the Client Environment that Databit reasonably determines creates a serious security risk. Databit will exercise its right to terminate without cause in good faith and not to avoid obligations it has already incurred. If Databit terminates without cause: (A) on Client's written request delivered before the termination date, Databit will continue to provide the Services for up to sixty (60) additional days at the then-current Fees to allow Client to transition; (B) no Project Migration Fee applies; and (C) Databit will refund any prepaid Fees for Services not performed. Except as stated in this Section, Databit has no liability to Client for terminating under this Section.

7.6 **Termination by Client for Cause.** Client may terminate an Engagement Document on written notice if Databit materially breaches it and does not cure the breach within thirty (30) days after receiving written notice describing the breach in reasonable detail. In that case the 180-day Notice Period payment in Section 7.4 does not apply, but Client remains responsible for Fees for Services performed and for non-cancellable Third-Party Services commitments.

7.7 **Effect of Termination.** On termination of an Engagement Document: (a) all unpaid Fees for Services performed, Fees for the Notice Period, non-cancellable Third-Party Services commitments and any Project Migration Fee become due on the effective date of termination; (b) Databit will remove or disable its tools and agents; and (c) Databit may delete Client Data from Databit-controlled systems as described in Section 7.9. Termination of one Engagement Document does not terminate others unless the notice says so.

7.8 **Transition and Migration Services.** On request, Databit will provide reasonable assistance to transition Services to Client or a new provider, which may include data export, documentation handover, transfer of administrative access, removal of Databit tools and coordination with the new provider ("Migration Services"). If Client moves any Services, systems, users or data to another provider, whether in whole or in part, Client will pay the Project Migration Fee stated in the applicable Engagement Document for the Migration Services. No Project Migration Fee applies if Databit terminates without cause under Section 7.5(a) or Client terminates for Databit's breach under Section 7.6; in those cases, Migration Services that Client requests are billed at Databit's then-current rates. Other transition work is billed at Databit's then-current rates, and Databit may require payment in advance.

7.9 **Credentials and Client Data on Exit.** Client Data is and remains Client's property. Databit will provide Client's Authorized Contact with the administrative credentials for Client-owned systems and tenants that Databit manages within a reasonable time after Client has paid all invoiced amounts in full, including amounts Client disputes, which Client may pay under protest without waiving its dispute. Until then, Databit will not change or revoke any administrative access Client already has or use its own access to deny Client access to Client-owned systems, and will release credentials earlier where reasonably necessary to respond to an active security incident or to comply with law. Regardless of payment status, Databit will make Client Data held in Databit-controlled systems available for export in its existing format for thirty (30) days after the effective date of termination. After that period, Databit may permanently delete Client Data from Databit-controlled systems without liability. Client Data held by Third-Party Providers is subject to their retention policies.

7.10 **Survival.** Sections 1, 5, 6.3, 7.7 through 7.10, 8, 9, 10.3, 11, 12, 13, 14 and 15, and any other provision that by its nature should survive, survive termination.

8. Data, Security and Privacy

8.1 **Client Data.** Client grants Databit a limited license to access, copy, process and transmit Client Data solely as needed to provide the Services, comply with law and enforce the Agreement.

8.2 **Databit Safeguards.** Databit will maintain reasonable administrative, technical and physical safeguards, appropriate to the nature of the Services, designed to protect Client Data in Databit-controlled systems, and will select Third-Party Providers that it reasonably believes maintain appropriate safeguards.

8.3 **Shared Responsibility.** Security depends on both parties and on Third-Party Providers. No security measure is perfect, and Databit does not guarantee that the Services will prevent all Security Incidents, malware, ransomware or unauthorized access. Client is responsible for its users' conduct, credentials and devices, and for decisions about security controls it declines under Section 3.8.

8.4 **Security Incidents.** Databit will notify Client without undue delay after confirming a Security Incident affecting Client Data in Databit-controlled systems and will provide information reasonably available to Databit to help Client meet its obligations. As the owner of Client Data, Client is responsible for any notices to individuals, regulators or others. Incident response, forensic and recovery work is out of scope unless the Security Incident was caused by Databit's breach of Section 8.2.

8.5 **Processing of Personal Data.** To the extent Databit processes Personal Data on Client's behalf as a processor or service provider under applicable law (including the New Jersey Data Privacy Act), Databit will: (a) process it only on Client's documented instructions, which are the Agreement and Client's reasonable written requests; (b) ensure that persons processing it are subject to a duty of confidentiality; (c) engage subcontractors that process Personal Data only under written contracts requiring them to meet the obligations of this Section; (d) provide reasonable assistance

with data-subject requests, security obligations and data-protection assessments, at Databit's then-current rates where the assistance goes beyond the Services; (e) delete or return Personal Data at the end of the Services as described in Section 7.9, unless retention is required by law; and (f) make available information reasonably necessary to demonstrate compliance with this Section. The Agreement describes the nature, purpose and duration of processing; the types of Personal Data are those Client places in the Client Environment.

8.6 **Regulated Data.** Client will tell Databit in writing before Databit is given access to data regulated under HIPAA, the Gramm-Leach-Bliley Act, 23 NYCRR Part 500, PCI DSS or similar regimes. The parties will sign any addendum reasonably required (such as a business associate agreement). Until then, Databit is not responsible for requirements specific to that regime.

8.7 **Monitoring and Authority.** Client authorizes Databit to access and monitor the Client Environment, including endpoints, networks and email systems, as needed to provide the Services. Client represents that it has the authority to grant that access and will give any notices to, and obtain any consents from, its employees and users that applicable law requires, including employee electronic-monitoring notices.

8.8 **Service Data.** Databit may use Service Data, and aggregated or de-identified data that does not identify Client or any individual, to operate, secure and improve its services.

9. Confidentiality

9.1 **Definition.** "Confidential Information" means non-public information disclosed by one party ("Discloser") to the other ("Recipient") that is marked confidential or that a reasonable person would understand to be confidential, including Client Data, system credentials, network designs, pricing and the terms of the Agreement. It does not include information that (a) is or becomes public through no fault of Recipient; (b) Recipient already knew without a duty of confidentiality; (c) Recipient lawfully receives from a third party without a duty of confidentiality; or (d) Recipient develops independently.

9.2 **Obligations.** Recipient will use Discloser's Confidential Information only to perform or receive the Services or enforce the Agreement, protect it with at least reasonable care, and disclose it only to its personnel, subcontractors, Third-Party Providers and advisers who need to know it and are bound by confidentiality obligations at least as protective as this Section.

9.3 **Credentials.** Databit will keep administrative passwords and credentials for the Client Environment confidential and will not release them to third parties without Client's written consent, except to Client's Authorized Contacts or as required by Section 7.9 or by law.

9.4 **Compelled Disclosure.** Recipient may disclose Confidential Information if required by law or court order, after giving Discloser prompt notice where legally permitted and reasonable cooperation in seeking protective treatment.

9.5 **Duration.** These obligations continue during the term and for three (3) years after it ends, and for trade secrets and Client Data, for as long as they remain protected by law.

10. Warranties and Disclaimers

10.1 **Mutual.** Each party represents that it has authority to enter into the Agreement and that the person signing for it is authorized to do so.

10.2 **Services Warranty.** Databit warrants that it will perform the Services in a professional and workmanlike manner consistent with generally accepted industry practices. Client must notify Databit of any breach of this warranty within thirty (30) days after the affected Services were performed. Client's exclusive remedy, and Databit's sole obligation, is for Databit to re-perform the nonconforming Services or, if Databit cannot do so within a reasonable time, to refund the Fees paid for them.

10.3 **Disclaimer. EXCEPT AS EXPRESSLY STATED IN SECTION 10.2, THE SERVICES AND ALL THIRD-PARTY SERVICES ARE PROVIDED "AS IS" AND DATABIT DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. DATABIT DOES NOT WARRANT THAT THE SERVICES OR ANY THIRD-PARTY SERVICES WILL BE UNINTERRUPTED, ERROR-FREE OR SECURE, THAT ALL DEFECTS WILL BE CORRECTED, THAT DATA WILL NOT BE LOST, OR THAT THE SERVICES WILL ACHIEVE ANY PARTICULAR SECURITY OR REGULATORY OUTCOME.**

11. Limitation of Liability

11.1 **Excluded Damages. EXCEPT FOR EXCLUDED CLAIMS, NEITHER PARTY IS LIABLE TO THE OTHER, UNDER ANY THEORY (INCLUDING CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR STATUTE), FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, OR FOR LOST PROFITS, LOST REVENUE, BUSINESS INTERRUPTION, LOSS OF GOODWILL, LOSS OR CORRUPTION OF DATA, COST OF RECREATING DATA, COST OF SUBSTITUTE SERVICES OR RANSOM PAYMENTS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

11.2 **Liability Cap. EXCEPT FOR EXCLUDED CLAIMS, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THE AGREEMENT WILL NOT EXCEED THE FEES PAID OR PAYABLE BY CLIENT TO DATABIT UNDER THE ENGAGEMENT DOCUMENT GIVING RISE TO THE CLAIM DURING THE TWELVE (12) MONTHS IMMEDIATELY BEFORE THE EVENT GIVING RISE TO THE CLAIM (OR, IF THE EVENT OCCURS DURING THE FIRST TWELVE (12) MONTHS OF THAT ENGAGEMENT DOCUMENT, THE FEES PAYABLE FOR ITS FIRST TWELVE (12) MONTHS), EXCLUDING AMOUNTS FOR THIRD-PARTY SERVICES THAT DATABIT PASSES THROUGH TO THIRD-PARTY PROVIDERS.**

11.3 **Excluded Claims.** "Excluded Claims" means: (a) Client's obligation to pay Fees; (b) a party's indemnification obligations under Section 12; (c) liability arising from a party's gross negligence, willful misconduct or fraud; (d) liability for bodily injury or death; and (e) any other liability that cannot be limited or excluded by law.

11.4 **Third-Party Providers.** Databit is not liable for the acts, omissions, outages, security failures or data loss of Third-Party Providers, other than subcontractors acting under Databit's direction under Section 3.4.

11.5 **Basis of the Bargain.** The parties agree that the Fees reflect the allocation of risk in this Section 11 and that these limitations apply even if a limited remedy fails of its essential purpose.

11.6 **Time to Bring Claims.** Except for claims to collect Fees, no claim arising out of the Agreement may be brought by either party more than one (1) year after the claiming party knew or reasonably should have known of the facts giving rise to the claim.

12. Indemnification

12.1 **By Client.** Client will defend, indemnify and hold harmless Databit and its officers, employees and subcontractors from third-party claims, and related losses, judgments, fines and reasonable attorneys' fees, arising from: (a) Client Data or Client's instructions to Databit; (b) use of the Services or Third-Party Services by Client or its users in violation of law, the Agreement or Third-Party Terms; (c) unlicensed or infringing software or content in the Client Environment not supplied by Databit; (d) Client's failure to give notices or obtain consents required by law; (e) claims by Client's employees, customers or users relating to the Services, except to the extent caused by Databit's negligence, gross negligence or willful misconduct; or (f) Client's refusal or failure to implement a security control or other measure that Databit recommended in writing.

12.2 **By Databit.** Databit will defend, indemnify and hold harmless Client from third-party claims, and related losses and reasonable attorneys' fees, for (a) bodily injury or damage to tangible property caused by the negligence or willful misconduct of Databit personnel while on Client premises; and (b) allegations that materials created by Databit (excluding Third-Party Services and Client-provided materials) infringe a third party's United States intellectual property rights.

12.3 **Procedure.** The indemnified party will give prompt written notice of the claim, allow the indemnifying party to control the defense and settlement (provided no settlement imposes obligations on the indemnified party without its consent, not to be unreasonably withheld), and provide reasonable cooperation at the indemnifying party's expense.

13. Non-Solicitation of Personnel

13.1 **Non-Solicitation.** During the term of any Engagement Document and for twelve (12) months after the last one ends, Client will not, directly or through others, solicit for employment or engagement any Databit employee or individual contractor who performed Services for Client during the preceding twelve (12) months ("Databit Personnel"). General advertisements not targeted at Databit Personnel are not solicitation.

13.2 **Placement Fee.** If, during that period, Client hires or engages any Databit Personnel, directly or through a staffing agency or other service provider to perform services for Client, whether or not solicited, Client will pay Databit a placement fee equal to thirty percent (30%) of the individual's annualized compensation at Databit, which the parties

agree is a reasonable estimate of Databit's recruiting, training and transition costs, consistent with customary recruiting fees, and not a penalty. Databit may seek injunctive relief for a threatened or continuing breach of Section 13.1.

14. Governing Law and Dispute Resolution

14.1 **Governing Law.** The Agreement is governed by the laws of the State of New Jersey, without regard to its conflict-of-laws rules.

14.2 **Informal Resolution.** Before starting litigation (other than to collect Fees or seek injunctive relief), a party will give the other written notice of the dispute, and senior representatives of both parties will meet (in person or virtually) within fifteen (15) days and try in good faith to resolve it within thirty (30) days of the notice.

14.3 **Venue.** Each party consents to the exclusive jurisdiction and venue of the state courts located in Bergen County, New Jersey, and the United States District Court for the District of New Jersey, for any action arising out of the Agreement, except that Databit may bring collection actions in any court with jurisdiction over Client.

14.4 **Jury Waiver. EACH PARTY KNOWINGLY AND VOLUNTARILY WAIVES ITS RIGHT TO A TRIAL BY JURY IN ANY ACTION OR PROCEEDING ARISING OUT OF OR RELATING TO THE AGREEMENT.**

14.5 **Attorneys' Fees.** Client will pay Databit's reasonable costs of collecting past-due Fees under Section 5.3. In any other action arising out of the Agreement, the prevailing party may recover its reasonable attorneys' fees and costs.

14.6 **Equitable Relief.** A breach of Section 9 or 13 may cause irreparable harm, and the non-breaching party may seek injunctive relief without posting a bond, in addition to other remedies.

15. General Terms

15.1 **Force Majeure.** Neither party is liable for delay or failure to perform (other than payment obligations) caused by events beyond its reasonable control, including natural disasters, fire, flood, power or internet failures, failures of Third-Party Providers, cyberattacks not caused by the affected party's failure to maintain reasonable safeguards, epidemics, labor disputes, war, terrorism and acts of government.

15.2 **Notices.** Notices of breach, termination, non-renewal or legal claims must be in writing and delivered by hand, nationally recognized courier or certified mail to the address in the Engagement Document, with a copy by email to the designated notice contact; they are effective on receipt. Operational notices, including notices of MSA updates, price changes and suspension, may be given by email, through the client portal or on invoices.

15.3 **Assignment.** Client may not assign the Agreement without Databit's prior written consent, which will not be unreasonably withheld. Databit may assign the Agreement to an affiliate or to a successor in a merger, acquisition or sale of all or substantially all of the relevant business.

15.4 **Independent Contractors.** The parties are independent contractors. Nothing in the Agreement creates a partnership, joint venture, agency or employment relationship.

15.5 **Good Faith.** Each party will act in good faith in performing its obligations under the Agreement.

15.6 **No Third-Party Beneficiaries.** The Agreement benefits only the parties and their permitted successors and assigns.

15.7 **Entire Agreement.** The Agreement is the entire agreement between the parties on its subject matter and supersedes all prior agreements, proposals and understandings, including any prior Databit Managed Services Agreement or Service Level Agreement, except for amounts already owed under them.

15.8 **Severability.** If any provision is held unenforceable, it will be enforced to the maximum extent permitted and modified to the minimum extent necessary to make it enforceable, and the remaining provisions remain in full force.

15.9 **Waiver.** A failure or delay in enforcing a provision is not a waiver. A waiver must be in writing.

15.10 **Interpretation.** Headings are for convenience only. "Including" means "including without limitation." The Agreement will not be construed against either party as drafter.

15.11 **Electronic Signatures and Counterparts.** Engagement Documents may be signed electronically and in counterparts, each of which is an original and all of which together are one instrument.

15.12 **Publicity.** Databit may identify Client by name as a customer in customer lists unless Client asks it not to in writing. Any other public statement about the relationship requires the other party's consent.

15.13 **Compliance with Law.** Each party will comply with laws applicable to its performance under the Agreement, including export control and sanctions laws.

Schedule 1 – Managed Services Service Standards

This Schedule applies to managed services provided under an Engagement Document. The Engagement Document controls if it states different coverage, response targets or rates.

S1. Hours of Coverage

Coverage window	Hours	Included?
Business Hours	Monday–Friday, 9:00 a.m.–5:00 p.m. Eastern, excluding Observed Holidays	Included for covered Services
After Hours	Monday–Friday, 5:00 p.m.–11:00 p.m. Eastern	As stated in the Engagement Document; otherwise billed at after-hours rates
Nights and Weekends	Monday–Friday, 11:00 p.m.–9:00 a.m.; Friday 11:00 p.m.–Monday 9:00 a.m.	As stated in the Engagement Document; otherwise billed at after-hours rates
Observed Holidays	See below	As stated in the Engagement Document; otherwise billed at after-hours rates

Observed Holidays: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day and Christmas Day. Automated monitoring runs continuously; alerts designated as critical are routed to Databit's on-call staff outside Business Hours.

S2. Priority Levels and Targets

	Priority 1 – Critical	Priority 2 – High	Priority 3 – Medium	Priority 4 – Low
Business impact	All or most work stopped; no acceptable workaround	Significant work stopped; short-term workaround only	Some work affected; workaround available	Minor impact or a request
Users affected (guide)	75–100%	30–75%	15–30%	0–15%
Response target	1 hour	2 hours	8 business hours	1 Business Day
Resolution target	24 hours from first response	36 hours from first response	5 Business Days from first response	30 days from first response

Databit assigns the priority level, taking into account cost, impact, severity and the availability of a workaround, and will reconsider it if Client asks. Targets are measured in Databit's ticketing system from ticket creation and apply only during covered hours.

S3. How Targets Are Measured; Exceptions

- Timers pause while Databit is waiting on Client, a Third-Party Provider or a manufacturer, and outside covered hours.
- Requests submitted by email may take several minutes to create a ticket; the client portal or desktop agent is the preferred method, and the phone line should be used for Priority 1 and 2 issues.
- Targets do not apply: during the first ninety (90) days of service while onboarding is in progress; to out-of-scope, after-hours or holiday work unless the Engagement Document includes it; to issues that require resolution by a Third-Party Provider; or where the user working with Databit is not the designated technical contact and cannot reasonably assist.

S4. Requesting Support and Escalation

Client users may request support through the client portal or desktop agent, by email to dbmshelpdesk@databitmsp.com, or by calling the Databit help desk directly at 201-479-9222. Databit's corporate office can be reached at 201-529-8050, and

current support information is published at www.databitinc.com. Databit may update these contact details by email notice or on its website. Requests should include the user's name and contact details, a description of the problem and any error messages, the number of users affected, whether a workaround exists, and any recent changes. Outside Business Hours, Client should call the help desk at 201-479-9222 and use the emergency option for urgent issues; Databit's on-call technician will confirm whether the request is in scope and, if it is not, will contact Client's after-hours Authorized Contact for approval before proceeding.

Requests begin with the service desk (Tier 1) and are escalated internally to systems engineers (Tier 2), senior engineers and Databit's vCIO (Tier 3) and, where needed, to Third-Party Provider support. Databit aims to keep one point of contact for each request. Client may ask Databit to re-evaluate a request's priority at any time.

S5. Onboarding

Onboarding normally takes 45 to 90 days and includes deploying Databit's tools, documenting the Client Environment, setting maintenance windows and Authorized Contacts, reviewing backups and security posture, and proposing a plan to bring the Client Environment up to the minimum standards below. Remediation work needed to meet those standards is out of scope unless included in the Engagement Document. Onboarding ends with a business review, normally around day 45.

S6. Minimum Standards

To be covered, the Client Environment must meet the following (Databit may update these standards on written notice as technology and threats change):

- Operating systems, firmware and business applications are on versions that receive security updates from the manufacturer or publisher.
- All software is genuine and properly licensed.
- Servers, workstations and laptops run Databit-approved endpoint detection and response (EDR) or antivirus protection.
- Multi-factor authentication is enabled for email, remote access, administrative and cloud accounts.
- A business-grade, vendor-supported firewall protects each site, and wireless networks use current encryption.
- Business data is backed up by a monitored solution that includes an off-site or immutable copy.
- Workstations and network equipment are generally no more than five (5) years old and servers no more than six (6) years old, and critical hardware is under manufacturer warranty or support.
- Databit's monitoring agent is installed on each covered device, and covered devices have reliable internet connectivity.

S7. On-Site Services

Databit provides services remotely where practical. Databit will dispatch a technician on site when physical work is needed, remote access is not available, or Databit expects on-site work to be faster. Databit decides whether a dispatch is necessary. If Client requests an on-site visit that Databit reasonably considers unnecessary, out-of-scope rates and any dispatch fees in the Engagement Document apply. If Client refuses on-site work that Databit considers necessary, response and resolution targets no longer apply to that request.

S8. General Exclusions

Unless an Engagement Document expressly includes them, the Services do not cover:

- Costs of bringing the Client Environment up to the minimum standards.
- Hardware, parts, consumables, shipping, software, licenses, subscriptions and Third-Party Provider support or incident fees.
- Work on systems not covered by manufacturer warranty or support, or not listed as covered in the Engagement Document.

- Work made necessary by changes, installations or repairs by anyone other than Databit, by misuse, or by malicious acts of Client's users.
- Damage from accidents, theft, power events, water, lightning, environmental conditions or building changes.
- Projects, relocations, new site build-outs and major upgrades or migrations.
- Data recovery beyond the backup services purchased, and incident response, forensics and ransomware recovery except as stated in Section 8.4.
- Travel to locations not listed as covered, or travel beyond the limits stated in the Engagement Document.

If Databit finds after the fact that work it performed as covered was in fact excluded (for example, an issue caused by an unauthorized change), Databit may invoice that work at the applicable rates on the next monthly invoice.

S9. Client Service Responsibilities

- Agree maintenance windows with Databit during onboarding; Databit may perform planned maintenance and reboots during those windows without further approval.
- Designate at least one on-site technical contact, one approver and one after-hours contact, and keep their details current.
- Ask users to request support through the processes in S4 rather than contacting individual technicians.
- Participate in periodic (normally quarterly) reviews of service performance, backups and disaster recovery, security posture and technology planning.
- Respond promptly to requests for approvals, information and access; Databit is not responsible for impacts caused by delayed approvals.

S10. Approval of Out-of-Scope Charges

Databit will obtain approval from an Authorized Contact before performing out-of-scope work expected to cost more than ten percent (10%) of Client's base monthly recurring Fees for that request. Client agrees to pay for out-of-scope work below that threshold without separate approval, but once out-of-scope charges in a calendar month total twenty-five percent (25%) of the base monthly recurring Fees, Databit will obtain approval for any further out-of-scope work that month. Approvals may be given by email, ticket or client portal. If Client declines a quote, Databit will propose an alternative where one exists or record the issue for discussion at the next review.