Last Revised: December 9, 2025

End-User License Agreement

THIS IS A LEGAL AGREEMENT BETWEEN CUSTOMER AND ENTERPRISEDB ("EDB") COVERING ITS PRODUCTS AND SERVICES. BY ACCESSING AND/OR USING THE PRODUCTS OR SERVICES, CUSTOMER IS AGREEING, ON BEHALF OF A LEGAL ENTITY ("CUSTOMER"), TO BE BOUND BY THE TERMS OF THIS AGREEMENT. THIS AGREEMENT DOES NOT APPLY TO ANY THIRD PARTY PRODUCTS OR SERVICES SOLD BY EDB, WHICH SHALL BE SUBJECT TO THE TERMS OF THE THIRD PARTY PROVIDER.

1. **DEFINITIONS**. As used in this Agreement, the following defined terms shall apply:

1.1. **Affiliate** means, with respect to either party, any person, firm, corporation, trust or other entity or combination thereof which directly or indirectly controls, is controlled by, or is under common control with such party; the term "control" meaning an ownership of greater than fifty percent (50%) of the voting and equity rights, of such person, firm, trust, corporation, or other entity (or combination thereof) or the power to direct the management of such person, firm, trust, corporation, or other entity (or combination thereof).

1.2. **Agreement** means this agreement, and any other documents incorporated herein by reference.

1.3. **Customer Account** means an account for Customer that is required to access and utilize Cloud Services.

1.4. **Customer Content** means any data uploaded to Customer's Account for storage, or data in Customer's computing environment to which EDB is provided access in order to provide Cloud Services or EDB Services. Customer Content shall be treated as confidential information subject to the standard of care set forth in Section 9.7.

1.5. **Cloud Services** means EDB software-as-a-service offerings inclusive of any services delivered through any unified, hosted EDB service delivery platform, including any on-premises components (e.g., client software, tools, on-premises software), and Updates, all as further described in the Documentation. EDB may update the Cloud Services with Updates at any time in its sole discretion. Support Services are included in a Cloud Services subscription.

1.6. **Deliverables** means any deliverables from EDB Services, including but not limited to consulting deliverables and Training Materials.

1.7. **Documentation** means manuals, instructions, and other documents and materials that EDB provides with EDB Products or Deliverables which describe the functionality, components, features or requirements of EDB Products or Deliverables, as amended from time to time.

1.8. **EDB Products** means proprietary Software or Cloud Services made available by EDB to Customer pursuant to this Agreement under an applicable Order, together with Updates and any associated Documentation.

1.9. **EDB Services** means Professional Services and Support Services made available by EDB to Customer pursuant to this Agreement under an applicable Order.

1.10. **EnterpriseDB** or **EDB** means the EDB contracting entity specified in Section 9.19.

1.11. **Entitlement** means the purchased EDB Products or EDB Services entitlement(s) under the license and delivery model(s) by which EDB measures, prices and offers the EDB Products and EDB Services to Customer. Entitlements to EDB Products or EDB Services subscriptions are limited to a Subscription Term.

1.12. **Fees** means all EDB fees applicable to EDB.

1.13. **Infringement Claim** means any claim, suit or proceeding brought against Customer based on an allegation that EDB Products, EDB Services or Deliverables, as delivered by EDB, infringe upon any patent or copyright or violate any trade secret rights of any third party.

1.14. **Logs** means records of Cloud Services and Support Services, including, but not limited to, information on performance, stability, usage, security, support, and technical information about devices, systems, related software, services or peripherals associated with Customer's use of Cloud Services and Support Services.

1.15. **Open Source Software** means any open source software provided by EDB in Software or a Deliverable. Open Source Software in Software will be described in the license directory for the Software and identified in the Deliverable. Notwithstanding any other provision of this Agreement, Open Source Software is licensed exclusively under the applicable open source license. PostgreSQL license terms are at https://www.postgresql.org/about/licence/.

1.16. **Order** means any initial or subsequent ordering document (including, but not limited to, a purchase order, order form, or signed proposal or statement of work), auto-renewal (if applicable, and you have not provided

notice of non-renewal), and/or online request for access to and/or use of the EDB Products or EDB Services submitted to EDB, an EDB authorized reseller, and/or through authorized marketplace websites.

1.17. **Professional Services** means any professional services (including, but not limited to, consulting and training), made available by EDB to Customer pursuant to this Agreement under an applicable Order. Professional Services must be used within the timeframe indicated by the SKU, or if there is a statement of work, as indicated by the statement of work. If no timeframe is indicated, Professional Services must be used within six (6) months of purchase. If not used within such timeframe, the Professional Services will be forfeited.

1.18. **Security Incident** means unauthorized access to Customer Content resulting in the loss of confidentiality, integrity or availability.

1.19. **Software** means EDB's proprietary programs in object code form made available by EDB to Customer pursuant to this Agreement under an applicable Order, together with Updates and any associated Documentation. Support Services are included in a Software subscription.

1.20. **Subscription Term** means the term for which EDB Products or EDB Services are licensed or made available by EDB to Customer pursuant to this Agreement under an Order, if applicable.

1.21. **Support Services** means EDB's delivery of technical support services for Software or Cloud Services under the services identified at EDB Postgres AI Plans and SLO Support Terms or management and monitoring services described at Enterprise Packaged Services Deliverables and Remote DBA and Service Monitoring. Support Services are included in Software and Cloud Services subscriptions and may otherwise be purchased standalone.

1.22. **Training Materials** means EDB's training courses, course curricula, course descriptions, course materials, and any other documentation or information, in any form or medium, furnished by EDB in connection with Training Services. Training Materials are Deliverables.

1.23. **Training Services** means EDB training services made available by EDB to Customer pursuant to an Order.

1.24. **Taxes** means all applicable transactional taxes on EDB Products and EDB Services (including but not limited to withholding tax, sales tax, services tax, value-added tax (VAT), goods and services tax (GST), and tariffs and/or duties) imposed by any government entity or collecting agency based on purchase.

1.25. **Update** means any corrections, bug fixes, features or functions added to or removed from the Products if and when made generally available by EDB during a Subscription Term. Updates are included in EDB Product subscriptions.

1.26. **User** means an individual that is authorized by Customer to access Software or Cloud Services under the Customer's Entitlement.

2. **RIGHTS**.

2.1. **Right to Use Software.** EDB hereby grants Customer a limited, personal, non-exclusive, non-transferable, worldwide license to use the Software under a purchased subscription for internal use in accordance with the Customer's Entitlement and the Documentation. At the conclusion of a Software subscription, if not renewed, Customer agrees to de-install the Software and to cease use of it.

2.2. **Right to Use Cloud Services**. EDB hereby grants Customer a limited, personal, non-exclusive, non-transferable, worldwide license to use the Cloud Services under a purchased subscription for internal use in accordance with Customer's Entitlement and the Documentation. Except to the extent permitted by applicable law, Customer agrees not to (**i**) knowingly or negligently access or use the Cloud Services in a manner that abuses or disrupts the EDB networks, security systems, customer accounts, or the Cloud Services, or any third party; (**ii**) attempt to gain unauthorized access to any of the above through unauthorized means; or (**iii**) transmit through or post on the Cloud Services any material that is deemed abusive, harassing, obscene, slanderous, fraudulent, libelous or otherwise unlawful. If Customer becomes aware or receives notice from EDB that any Customer Content or any User's access to or use of Customer Content violates this Section, Customer must take immediate action to remove the applicable part of the Customer Content. EDB may ask Customer to remediate, and if Customer fails to comply with such request, EDB may suspend the Cloud Service pursuant to Section 9.10.

2.3. **Right to Use EDB Services**. EDB grants to Customer a limited, personal, non-exclusive, non-transferable, worldwide license to use Support Services, Professional Services and Deliverables under a purchased subscription or other engagement model in accordance with the Customer's Entitlement for internal use. All intellectual property rights in all Deliverables, pre-existing works and derivative works of such pre-existing works, as well as developments made, conceived, created, discovered, invented, or reduced to practice in the performance of the Professional Services, are and shall remain the sole and absolute property of EDB.

2.4. **Limitations on Use**. Customer agrees not to; (**i**) modify, distribute, prepare derivative works of, reverse engineer, reverse assemble, disassemble, decompile or attempt to decipher any code relating to Software, Cloud Services or Deliverables; (**ii**) market, offer to lease, sell, and/or resell the Software, Cloud Services

or Deliverables or use them for service bureau or time sharing or in any other way allow third parties to exploit them; or (**iii**) if the Customer is an EDB competitor, use the Software, Cloud Services or Deliverables directly or indirectly for competitive development, benchmarking or analysis, except to the extent permitted under applicable law. Customer may allow Affiliates to use EDB Products, Services and Deliverables under its Entitlement provided Customer binds them under this Agreement and remains responsible for any breach from their acts or omissions.

2.5. **Proprietary Rights**. Except for the limited use rights expressly granted herein, Customer has no right, title or interest in or to EDB Products, EDB Services or Deliverables or any intellectual property rights related thereto.

3. **ORDERS, FEES AND PAYMENT**. Customer may order EDB Products or EDB Services using the EDB then-current ordering processes, including authorized reseller and online marketplace ordering processes, as applicable. Customer is responsible for all Fees on Orders in accordance with the GSA Schedule Pricelist. EDB shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k) and 52.229-1. Payment is due for an EDB Product or EDB Service for the Entitlement purchased, including any renewals, pursuant to the payment schedule of the associated SKU, including any applicable license model. If you purchase a multi-year subscription, or multi-year renewal, subject to the availability of multi-year funds and appropriations, your purchase is for the full value of all years of the Subscription Term, even if required payments are annual.. If you purchase a subscription under a consumption-based license model, your purchase constitutes your agreement to allow for reporting and be invoiced for and pay for consumption at intervals and pricing as defined in the license model. If your purchase includes a spending commitment, your purchase constitutes your agreement to be invoiced for and pay for the commitment as defined in the commitment model. **EDB or your EDB authorized reseller will provide a quote via e-mail of each subscription renewal at least ninety (90) days in advance of any renewal. If there is or has been an increase in your required Entitlement, you must provide notice to the party providing you with the quote. Increases can be pro-rated to align with the term of your current subscription. You must purchase additional licenses you have used from the date of initial use.** Unless you complete a subscription renewal through an EDB authorized reseller or marketplace, you understand and agree that the renewal will be invoiced by and payable to EDB. Fees may increase and discounts may not apply to renewals in accordance with the GSA Schedule Pricelist. A reinstatement Fee shall apply to reinstate a subscription which has lapsed. This Fee is in addition to the Fee for a new subscription for a new Subscription Term which must be purchased at the same time. The reinstatement Fee shall be equal to the amount that would have been paid from the date that the subscription lapsed until the reinstatement date. Payments to EDB are due net thirty (30) days after the receipt date of its invoice. Late payments will be subject to an interest rate. established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. EDB reserves the right to suspend an EDB Product or EDB Service subscription or any portion thereof for non-payment of Fees pursuant to Section 9.10 or terminate pursuant to Section 4.2.

4. **TERM AND TERMINATION**.

4.1. **Term**. Unless terminated earlier, this Agreement shall extend until the expiration of the last to expire of any Subscription Terms purchased hereunder (the “Term”).

4.2. **Termination for Cause**. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, EDB shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. In the event of termination by Customer for cause, Customer shall be entitled to a refund of any unused prepaid Fees, and relief from any subsequent subscription payments due for the remainder of the Subscription Term, with respect to such subscription

4.3. **Effect of Termination**. Upon termination, Customer will immediately discontinue all access and use of the relevant EDB Software or Cloud Service or EDB Service. Neither party shall be liable for any damages resulting from termination, including without limitation, unavailability of Customer Content arising therefrom; provided, however, termination shall not affect any claim, including, but not limited to Customer payment obligations, arising prior to the effective termination date. Customer may download Customer Content from a terminated Cloud Service subscription as set forth in Section 5.1.

5. **CUSTOMER CONTENT AND CUSTOMER ACCOUNT**.

5.1. **Customer Content.** Customer retains all rights to any and all of its Customer Content, subject to a non-exclusive, worldwide, royalty-free, license to EDB as necessary to provide Cloud Services and EDB Services hereunder. Each party shall apply reasonable technical, organizational and administrative security measures, as appropriate relative to Cloud Services and EDB Services, to keep Customer Content protected in accordance with industry standards as identified in Section 9.7. Cloud Service interaction with Customer

Content varies depending on the nature of the Cloud Service. If EDB reasonably believes a problem with the Cloud Service may be attributable to Customer Content or Customer's configuration or use of the Cloud Service, Customer shall cooperate with EDB to identify the source of and to resolve the problem. Customer shall comply with all intellectual property laws and obligations related to the Customer Content, as well as all legal duties applicable to Customer by virtue of using the Cloud Service, including providing all required information and notices and obtaining all required consents. EDB's exclusive obligations with respect to care of Customer Content are as expressly set forth herein. For Cloud Services that provide for download of Customer Content, Customer shall have thirty (30) days to download Customer Content after expiration or termination of the Cloud Service subscription and must contact EDB Support Services for download access and instructions. Except for the foregoing, EDB has no obligation to maintain Customer Content following expiration or termination of the Agreement (or Customer's Account for the affected Cloud Service).

5.2. **Customer Account**. Customer is solely responsible for (**i**) the configuration of Customer's Account; (**ii**) the operation, performance and security of Customer's equipment, networks and other computing resources used to connect to the Cloud Service; (**iii**) ensuring all Users exit or log off from the Cloud Service at the end of each session in accordance with Customer's session policy; (**iv**) maintaining the confidentiality of Customer's Account, User id's, conference codes, passwords and/or personal identification numbers used in conjunction with the Cloud Service, including not sharing login information among Users; and (**v**) all uses of the Service that occur using Customer's Account. Customer will notify EDB immediately of any unauthorized use of its Account or any other breach of security. Ownership of Customer's Account is directly linked to the individual or entity that completes the registration process for the Account. Customer acknowledges that EDB will rely on the information provided for issues arising with the Customer Account.

5.3. **Customer Account Access/Instructions**. The Customer Account owner, and any authorized User, will have access to information in the Customer Account. EDB will not provide access to any other User at any time. Customer agrees that EDB may rely on instructions given by the Customer Account owner either through the Account dashboard or via email from the address on file for the Customer Account owner. Customer agrees not to request access to or information about an account that is not owned by the Customer. In the event of a dispute regarding Customer Account data, EDB will only release information to another party other than the Customer Account owner pursuant to a court order or other notarized waiver and release as determined by EDB.

6. **WARRANTIES AND WARRANTY DISCLAIMER**.

6.1. **Software Subscription Warranty**. EDB warrants that during the Subscription Term, the Software when used in accordance with the Documentation will materially conform to the specifications in the Documentation, and Support Services will be delivered in a professional manner but that does not mean that every question raised will be resolved in a certain amount of time. EDB further warrants that it will employ commercially reasonable efforts in accordance with industry standards to detect and remove malware or malicious code from Software prior to delivery. EDB's entire liability and your exclusive remedy will be (**i**) replacement of the Software with conforming Software or provision of conforming Support Services, and if that is not possible or commercially practicable, (**ii**) termination of the subscription and provision of a prorated refund of any unused pre-paid Fees for the subscription from the date of non-conformance, and relief from any subsequent subscription payments due for the remainder of the Subscription Term.

6.2. **Cloud Services Warranty**. EDB warrants that during the Subscription Term, the Cloud Service, when used in accordance with the Documentation, will materially conform to the specifications in the Documentation, and Support Services will be delivered in a professional manner but that does not mean that every question raised will be resolved in a certain amount of time. EDB further warrants it will employ commercially reasonable efforts in accordance with industry standards to prevent the transmission of malware or malicious code via the Cloud Services. EDB's entire liability and your exclusive remedy will be (**i**) provision of a conforming Cloud Service or provision conforming Support Services, and if that is not possible or commercially practicable, (**ii**) termination of the subscription and provision of a prorated refund of any unused pre-paid Fees for the subscription from the date of non-conformance, and relief from any subsequent subscription payments due for the remainder of the Subscription Term.

6.3. **Support Services Subscription Warranty**. EDB warrants that during the Subscription Term, Support Services purchased as a standalone subscription will be delivered in a professional manner, but that does not mean that every question raised will be resolved in a certain amount of time. EDB's entire liability and your exclusive remedy will be (**i**) provision of conforming Support Services, and if that is not possible or commercially practicable, (**ii**) termination of the subscription and provision of a prorated refund of any unused pre-paid Fees for the subscription from the date of non-conformance, and relief from any subsequent subscription payments due for the remainder of the Subscription Term.

6.4. **Professional Services Warranty**. Professional Services will be delivered in a professional manner and Deliverables will materially conform to the specifications of the applicable SKU, but that does not include a commitment to achieve a particular outcome or results. EDB's entire liability and your exclusive remedy will be (**i**) re-performance of the Professional Services, and if that is not possible or commercially practicable, (**ii**) provision of a prorated refund of any pre-paid Fees for the non-conforming Professional Services. Customer agrees to reasonably cooperate with re-performance. Warranty claims for Professional Services

must be made in writing within ten (10) days of your receipt of any non-conforming Professional Services or Deliverables.

6.5. **Warranty Disclaimer**. THE FOREGOING LIMITED WARRANTIES DO NOT COVER PROBLEMS ARISING BY ACCIDENT, ABUSE OR USE IN A MANNER INCONSISTENT WITH THIS AGREEMENT OR RESULTING FROM EVENTS BEYOND EDB'S REASONABLE CONTROL, INCLUDING, WITHOUT LIMITATION, UNAVAILABILITY OF OR OPERATION IN COMBINATION WITH A THIRD PARTY NETWORK OR SYSTEM, HARDWARE, SOFTWARE, SERVICE OR DATA. TO THE EXTENT PERMITTED BY APPLICABLE LAW, EDB DISCLAIMS ALL OTHER REPRESENTATIONS, WARRANTIES AND CONDITIONS, WHETHER IMPLICATION, ESTOPPEL OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, QUIET ENJOYMENT, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, AND ANY CONDITIONS OF QUALITY, AVAILABILITY, RELIABILITY, SECURITY, OR BUGS OR ERRORS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES AND CONDITIONS, THEREFORE SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY IF CUSTOMER IS LOCATED IN SUCH A JURISDICTION. CUSTOMER IS RESPONSIBLE FOR THE SELECTION AND USE OF EDB PRODUCTS AND EDB SERVICES.

7. **INDEMNIFICATION BY EDB**. EDB shall indemnify and have the right to intervene to defend Customer against any third party Infringement Claim, and pay reasonable attorneys' fees, court costs, damages finally awarded, or reasonable settlement costs, with respect to such Infringement Claim; provided that: (**i**) Customer promptly notifies EDB in writing of an Infringement Claim such that EDB is not prejudiced by any delay of such notification; (**ii**) EDB has sole control over the defense and any settlement of any Infringement Claim; and (**iii**) Customer provides reasonable assistance in the defense of same. If Customer's use of any of the EDB Products, EDB Services or Deliverables is, or in EDB's opinion is likely to be, enjoined as a result of an Infringement Claim, EDB shall, at its sole option and expense, either (**i**) procure for Customer the right to continue to use them as contemplated herein, or (**ii**) replace or modify them to make their use non-infringing without degradation in performance or a material reduction in functionality. If options (**i**) and (**ii**) are not reasonably available, EDB may, in its sole discretion and upon written notice to Customer, require return of the relevant EDB Products or Deliverables, or cancel access to the relevant EDB Services, and refund to Customer any unused pre-paid Fees for the relevant Subscription Term or EDB Services, and provide relief from any subsequent subscription payments due for the remainder of the Subscription Term. EDB assumes no liability, and shall have no liability, for any Infringement Claim to the extent based on (**i**) Customer's access to and/or use of the EDB Products, EDB Services or Deliverables following notice of an Infringement Claim; (**ii**) any modification of the EDB Products, EDB Services or Deliverables by Customer or at its direction; (**iii**) Customer's combination of the EDB Products, EDB Services or Deliverables with third party programs, services, data, hardware, or other materials; (**iv**) Open Source Software in Software or Deliverables; or (**v**) any trademark or copyright infringement involving any marking or branding not applied by EDB or involving any marking or branding applied at Customer's request. THE FOREGOING STATES EDB'S SOLE LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY WITH RESPECT TO ANY INFRINGEMENT CLAIM HEREUNDER.

8. **LIMITATION OF LIABILITY**. EXCEPT FOR A BREACH BY CUSTOMER OF SECTION 2, INDEMNIFICATION BY EDB UNDER SECTION 7, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES OR LOSSES, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, THOSE ARISING OUT OF OR RELATING TO: (**i**) LOSS OF DATA; (**ii**) LOSS OF INCOME; (**iii**) LOSS OF OPPORTUNITY; (**iv**) LOST PROFITS; OR (**v**) UNAVAILABILITY (EXCLUDING CREDITS DUE FOR ANY EDB SERVICE LEVEL AGREEMENT OBLIGATION) OR NON-PERFORMANCE OF ANY OR ALL OF THE EDB PRODUCTS OR EDB SERVICES, IN EACH CASE, HOWEVER CAUSED, AND BASED ON ANY THEORY OF LIABILITY, INCLUDING, BUT NOT LIMITED TO, BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR VIOLATION OF STATUTE, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO SOME OF THE ABOVE LIMITATIONS MAY NOT APPLY. EXCEPT FOR A BREACH BY CUSTOMER OF SECTION 2, INDEMNIFICATION BY EDB UNDER SECTION 7, OR A SECURITY INCIDENT TO THE EXTENT CAUSED BY EDB'S BREACH OF THE EDB SECURITY EXHIBIT OR EDB DATA PROCESSING ADDENDUM, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE TOTAL CUMULATIVE LIABILITY OF EITHER PARTY TO THE OTHER OR ANY OTHER PERSON ARISING OUT OF THIS AGREEMENT AND/OR THE TERMINATION THEREOF, SHALL BE LIMITED TO THE SUM OF THE AMOUNTS PAID FOR THE APPLICABLE SOFTWARE OR CLOUD SERVICE DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE INCIDENT GIVING RISE TO THE LIABILITY, OR IN THE CASE OF PROFESSIONAL SERVICES, THE AMOUNT PAID FOR THE APPLICABLE SERVICES (GENERAL CAP). IN THE CASE OF A SECURITY INCIDENT TO THE EXTENT CAUSED BY EDB'S BREACH OF THE EDB SECURITY EXHIBIT OR EDB DATA PROCESSING ADDENDUM, THE TOTAL CUMULATIVE LIABILITY OF EDB TO CUSTOMER SHALL BE LIMITED TO THE SUM OF 2X THE

AMOUNTS PAID FOR THE APPLICABLE SOFTWARE, CLOUD SERVICE OR SUPPORT SERVICES DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE INCIDENT GIVING RISE TO THE LIABILITY, OR IN THE CASE OF PROFESSIONAL SERVICES, 2X THE AMOUNT PAID FOR THE APPLICABLE SERVICE (SUPER CAP). IN NO EVENT SHALL EDB BE LIABLE FOR THE SAME EVENT UNDER BOTH THE GENERAL CAP AND THE SUPER CAP. SIMILARLY, THOSE CAPS SHALL NOT BE CUMULATIVE; IF THERE ARE ONE OR MORE CLAIMS SUBJECT TO EACH OF THOSE CAPS, THE MAXIMUM TOTAL LIABILITY FOR ALL CLAIMS IN THE AGGREGATE SHALL NOT EXCEED THE SUPER CAP. THE FOREGOING SHALL NOT LIMIT CUSTOMER'S OBLIGATIONS TO PAY ANY FEES AND/OR OTHER SUMS DUE UNDER ANY ORDER. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

9. **ADDITIONAL TERMS**.

9.1. **U.S. Government End-Users**. If Customer is a U.S. Government agency, Customer hereby acknowledges and agrees that Software and the software being accessed through Cloud Services, as well as any client software that is downloaded by any User in connection with a Cloud Service, constitutes "Commercial Computer Software" as defined in Section 2.101 of the Federal Acquisition Regulation ("FAR"), 48 CFR 2.101. Therefore, in accordance with Section 12.212 of the FAR (48 CFR 12.212), and Sections 227.7202-1 and 227.7202-3 of the Defense Federal Acquisition Regulation Supplement ("DFARS") (48 CFR 227.7202-1 and 227.7202-3), the use, duplication, and disclosure of the software and related Documentation by the U.S. Government or any of its agencies is governed by, and is subject to, all of the terms, conditions, restrictions, and limitations set forth in this Agreement. If, for any reason, FAR 12.212 or DFARS 227.7202-1 or 227.7202-3 or these license terms are deemed not applicable, Customer hereby acknowledges that the Government's right to use, duplicate, or disclose the Software or other software and related Documentation are "Restricted Rights" as defined in 48 CFR Section 52.227-14(a) (May 2014) or DFARS 252.227-7014(a)(15) (Feb 2014), as applicable. Manufacturer is EnterpriseDB Corporation, 221 W. 9th Street, Wilmington, DE 19801, U.S.A.

9.2. **Australian Consumers**. EDB offerings come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the EDB offerings repaired or replaced if the offerings fail to be of acceptable quality and the failure does not amount to a major failure. Notwithstanding any other provision of this Agreement and to the extent permitted by applicable law, EDB's liability arising from or in relation to a claim under or a breach of any warranty or statutory guarantee that cannot be excluded will be limited, at EDB's option to: (**i**) the supplying of the Cloud Services or EDB Services again; or (**ii)** the payment of the cost of having the Cloud Services or EDB Services supplied again.

9.3. **Trial and Freemium**. If an EDB Product offering is identified as a trial, Customer may use the EDB Product for a limited period for internal demonstration, test, or evaluation purposes. If an EDB Product is offered as a freemium offering, Customer may use the EDB Product for production purposes during the term of the offering. EDB PROVIDES TRIALS AND FREEMIUM OFFERINGS "AS IS" AND WITHOUT WARRANTY. ANY CUSTOMER DATA UPLOADED IN A CLOUD SERVICES TRIAL OR FREEMIUM OFFERING WILL BE PERMANENTLY LOST UNLESS CUSTOMER PURCHASES A SUBSCRIPTION TO THE SAME CLOUD SERVICE AS COVERED BY THE TRIAL OR FREEMIUM OFFERING AT THE CONCLUSION OF ITS TERM OR EXPORTS SUCH DATA BEFORE SUCH DATE.

9.4. **Beta, Tech Preview and Free Tools.** EDB Products do not include Beta, Tech Preview or free tools offerings. Customer may use any software or cloud service identified as Beta or Tech Preview for internal demonstration, test or evaluation purposes for the term of the Beta or Tech Preview offering. Customer may use any software or cloud service identified as a free tool for test, evaluation or production purposes. CUSTOMER ACKNOWLEDGES THAT ANY SUCH SOFTWARE OR CLOUD SERVICE IS OFFERED "AS-IS" AND WITHOUT WARRANTY. SUCH SOFTWARE OR CLOUD SERVICE MAY CONTAIN BUGS, ERRORS AND OTHER DEFECTS. EDB has no obligation to provide Updates or Support Services or continued availability, and such offerings can be suspended or terminated at any time by EDB at its sole discretion without notice. EDB does not make any representations, promises or guarantees that Beta and Tech Preview offerings will be publicly announced or made generally available as EDB Products.

9.5. **Third Party Products, Services or Content**. A Cloud Service may contain features or functions that enable interoperation with third party products, services or content. EDB may also provide access to third party products, services or content directly within the Cloud Service. Third party products, services or content, and Customer content in third party services, are not part of the Services and are not warranted or supported by EDB. Your use of such third party products, services or content is subject to the terms of the third party, not EDB.

9.6. **Consent to Use Logs**. EDB and its service providers may collect and use Logs for purposes of facilitating Cloud Services and Support Services, including securing, managing, measuring and improving Cloud Services and Support Services. Logs may be used for purposes not specified in this Section only in an aggregated, anonymized form.

9.7. **Security and Privacy**. When providing Cloud Services or EDB Services, EDB will (i) implement and maintain the administrative, physical and technical security controls as set forth in the EDB Security Exhibit attached hereto and at https://trust.enterprisedb.com/?itemUid=7680ef28-a3b8-4516-bd4c-530178baf3db and (ii) process personal data on Customer's behalf as set forth in the EDB Data Processing Addendum attached hereto and at https://www.enterprisedb.com/data-processing-addendum. If Customer's use of EDB Products and EDB Services is subject to the European Union Digital Resilience Act ("DORA"), the DORA Addendum at https://trust.enterprisedb.com/?itemUid=b62b4957-cc7b-48b2-a3b2-eb12372d084d also applies. The EDB Services Security Exhibit, EDB Data Processing Addendum and DORA Addendum are incorporated herein by reference, as applicable. Customer agrees to provide any notices, obtain any consents or otherwise establish the legal basis necessary for EDB to access and process personal and other data as specified in this Agreement. Except as may be specifically identified in the Documentation for a particular offering, EDB Products and EDB Services are not designed for, and do not support, personal health information as covered by US HIPAA regulations.

9.8. **Cloud Service Infrastructure**. Cloud Services may be hosted on public or EDB private clouds. EDB may change cloud providers and/or clouds at its discretion but will provide at least thirty (30) days' notice of such a change and will use reasonable efforts to reduce any impact on availability of Cloud Services. Cloud Services are generally available 7/24/365, except during scheduled maintenance performed after contiguous U.S. business hours or on U.S. federal holidays. EDB will provide notice of any emergency maintenance or Updates that may impact availability during normal business hours.

9.9 **Cloud Services Service Level.** The EDB Service Level Agreement for Cloud Services is attached hereto and at https://www.enterprisedb.com/service-level-agreement-edb-postgres-ai. Your exclusive remedy for breach of service level commitments in the EDB Service Level Agreement is as identified therein. The EDB Service Level Agreement is incorporated herein by reference.

9.10. **Suspension of Service**. EDB reserves the right to suspend an EDB Product or EDB Service subscription if (**i**)reserved; (**ii**)reserved; (**iii**) Customer failed to timely address EDB's request to take action pursuant to Section 2.2; or (**iv**) suspension is required pursuant to a subpoena, court order or other legal process. EDB agrees to notify Customer of any such suspension. Customer will remain responsible for all fees incurred before or during any suspension.

9.11. **High-Risk Use**. Customer acknowledges that EDB Products are not designed or intended for use in life support systems, human implantation, nuclear facilities or any other application where Product failure could lead to loss of life or physical property damage.

9.12. **Voice and Data Charges; Customer Connectivity**. Customer is responsible for all fees and charges imposed by Customer's telephone carriers, wireless providers, and other voice and/or data transmission providers arising out of access to and use of EDB Products or EDB Services. If Customer's broadband connection and/or telephone service fails, or Customer experiences a power or other failure or interruption, Customer's access to Cloud Services or EDB Services may fail for reasons outside of EDB's control.

9.13. **Assignment**. Customer may not assign its rights or delegate its duties under this Agreement either in whole or in part without EDB's prior written consent, except that Customer may assign this Agreement in whole to an Affiliate, or a successor in interest as part of a corporate reorganization, consolidation, merger, or sale of all or substantially all of its assets. Customer shall provide notice to EDB upon completion of any permitted assignment. Any attempted assignment in violation of the foregoing shall be void. This Agreement will bind and inure to the benefit of each party's successors or permitted assigns.

9.14. **Export Restriction and Compliance with Laws**. Customer acknowledges that the EDB Products and EDB Services may be subject to U.S., foreign, and international export controls and economic sanctions laws and regulations and agrees to comply with all such applicable laws and regulations, including, but not limited to, the U.S. Export Administration Regulations ("EAR") and regulations promulgated by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"). Customer agrees not to, directly or indirectly, allow access to or use of the EDB Products or EDB Services in embargoed or sanctioned countries/regions, by sanctioned or denied persons, or for prohibited end-uses under U.S. law without authorization from the U.S. Government. Customer certifies that neither it nor any of its direct or indirect owners, officers, directors, controlling individuals or entities, employees, agents, or subcontractors (i) are included on any list of restricted or sanctioned parties maintained by the United States, European Union, United Kingdom, United Nations, or other applicable governmental authority; (ii) shall engage in any business dealings, directly or indirectly, in jurisdictions subject to comprehensive sanctions, or (iii) otherwise engage in violation of applicable sanctions. Both parties agree to comply with all other laws, rules and regulations applicable to that party or its activities hereunder.

9.15. **Compliance**. To the extent permitted by applicable law, and no more often than once each calendar year, EDB may request at its sole discretion that you self-report EDB Product usage or allow it to audit your usage. You agree to cooperate upon thirty (30) days' advance notice and during normal business hours. EDB will provide you with any necessary tools or assistance. If you are using an EDB Product with a compliance agent, you will implement the agent or provide manual reporting according to the Documentation to help

EDB track Product usage and ensure Product quality, security and performance. You agree to promptly notify EDB of incidents of non-compliance caused by your usage of EDB Products or EDB Services.

9.16. **Notices**. All legal notices required under this Agreement shall be in writing and delivered in person or by certified or registered express mail to the address last designated on the account for Customer, and the EDB contracting entity as specified below, or such other address as either party may specify by notice to the other party as provided herein. Notice shall be deemed given (**i**) upon personal delivery; (**ii**) if delivered by air courier or email, upon confirmation of receipt; or (**iii**) five (5) days after deposit in the mail. A copy of all legal notices from Customer to EDB must also be sent to legal-notices@enterprisedb.com. Non-legal notices under Section 3.0 or 9.8 may be provided to the other party's applicable email address and shall be deemed effective as of the date and time stamp on the email. EDB may also provide Customer with non-legal notices through its website and/or through in-product or in-service messaging or dashboards, which shall likewise be deemed effective immediately.

9.17. **Force Majeure**. In accordance with GSAR Clause 552.212-4(f), Neither party will be responsible or have any liability for any delay or failure to perform its non-monetary obligations hereunder to the extent due to unforeseen circumstances or causes beyond its reasonable control, including acts of God, earthquake, fire, flood, sanctions, embargoes, strikes, lockouts or other labor disturbances, civil unrest, failure, unavailability or delay of suppliers or licensors, riots, terrorist or other malicious or criminal acts, war, failure or interruption of the internet or third party internet connections or infrastructure, power failures, acts of civil and military authorities and severe weather. The affected party will give the other party prompt written notice of the failure to perform due to Force Majeure and use its reasonable efforts to limit the resulting delay in its performance.

9.18. **General Terms**. Captions and headings are used herein for convenience only, are not a part of this Agreement, and shall not be used in interpreting or construing this Agreement. The provisions of Sections 1 (Definitions), 2.4 (Limitations on Use), 2.5 (Proprietary Rights), 3 (Orders, Fees, and Payments), 4.3 (Effect of Termination), 5 (Customer Content and Customer Account), 7 (Indemnification by EDB), 8 (Limitation of Liability), 9.16 (Notices), 9.18 (General Terms), and 9.19 (EDB Contracting Entity, Choice of Law and Venue) shall survive any termination of the Agreement. If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, such provision shall be severed from this Agreement and the other provisions shall remain in full force and effect. The parties are independent contractors and nothing in this Agreement creates a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between or among the parties. EDB may subcontract responsibilities under this Agreement to Affiliates and/or third parties but remains responsible for breach of this Agreement by acts or omissions of such subcontractors. No person or entity not a party to this Agreement will be deemed to be a third party beneficiary of this Agreement or any provision hereof. EDB authorized resellers (including distributors) do not have the right to make modifications to this Agreement or to make any additional representations, commitments, or warranties binding on EDB. No waiver or amendment of any term or condition of this Agreement shall be valid or binding on any party unless agreed to in writing by such party. EDB's failure to enforce any term of this Agreement will not be construed as a waiver of the right to enforce any such terms in the future. Unless otherwise specified, remedies are cumulative.

9.19. **EDB Contracting Entity, Choice of Law and Venue**. The EDB contracting entity, relative to any dispute or claim arising out of or in connection with this Agreement, is: https://www.enterprisedb.com/edb-contracting-entities. This Agreement shall be governed by the Federal laws of the United States.

9.20. **Entire Agreement; Order of Precedence**. This Agreement sets forth the entire agreement and understanding of the parties relating to the subject matter hereof and supersedes all prior and contemporaneous oral and written agreements. Nothing contained in any Order or any other document or terms submitted by Customer with or as part of an Order, shall in any way add to or otherwise modify the Agreement or any EDB purchase program terms under which an Order is submitted. The terms of this Agreement or other referenced documents may be non-materially updated by EDB from time to time without notice (but will be posted on the EDB website and identified by a "Last Revised" date).

Service Level Agreement (SLA) - EDB Postgres AI Cloud Services

Introduction

This Service Level Agreement ("SLA") sets forth the applicable service levels and service level credits for Customer's use of EDB Postgres AI Cloud Services. The SLA service level credits are the Customer's exclusive remedy for EDB's failure to meet a specified service level.

This SLA is incorporated into the EDB EULA (https://www.enterprisedb.com/legal/EDB-Eula) (the "Agreement").

General Terms

Definitions

All terms capitalized will have the definition provided in the Agreement unless otherwise specified herein.

"Beta" or 'Tech Preview" refers to any service or feature that has been made available in pre-production release or on a testing basis.

"Cluster(s)" refers to the following types of clusters:

- **"Single Node Cluster" is a cluster without high availability enabled.**
- **"HA Cluster" or "High Availability Cluster" refers to a cluster with high availability enabled, not powered by EDB Postgres AI Distributed.**
- **"PGD Cluster" refers to a cluster powered by EDB Postgres AI Distributed, which may contain one or more Data Groups in a single or multiple regions.**

"Data Group" refers to a group of nodes in a single Region that are part of a PGD Cluster.

"Database Uptime" or "Uptime" is calculated in the following ways:

- **A minute is considered available if either: (a) there are no connections to the Cluster or Faraway Replica, or no active connections issuing queries; (b) there is at least one successful client connection established; or (c) an active connection issues a query to the Cluster or Faraway Replica.**
- **Minutes during which the Cluster or Faraway Replica is undergoing scheduled maintenance or upgrades are considered available.**
- **Single Node & HA Clusters or Faraway Replica availability is the total number of minutes during the month that the Cluster or Faraway Replica is available.**

- **PGD Cluster availability is the total number of minutes during the month that all Data Groups in the PGD Cluster are available.**

"Downtime" is calculated per Cluster or Faraway Replica on a monthly basis, and is the total number of minutes during the month that the Cluster or Faraway Replica is unavailable.

"Faraway Replica" refers to the faraway replica feature in EDB Postgres AI. Faraway replicas are read-only replicas of EDB Postgres AI Single Node or High Availability Clusters that you can provision in most supported Regions. Database users and applications can read from replicas instead of the source Cluster.

"Region" refers to the geographic area as defined by the applicable cloud service provider from which you deploy EDB Postgres AI, as the case may be.

"Service Credit" is calculated as a percentage of the charges paid by you for EDB Postgres AI for the month in the billing cycle in which the applicable SLA was not met.

"Service Level" refers to the applicable monthly Uptime percentage availability of a specified Cluster.

"Support" means the technical support and maintenance services as described in the then-current EDB Support Policy.

"Cloud Service Provider" or "CSP" is the infrastructure provider your databases live on - for example Amazon's AWS or Microsoft's Azure platforms.

Claims

In order for EDB to consider a claim for Service Credit, you must submit the claim within the prescribed time frame to the EDB Support Team at: cloudsupport@enterprisedb.com (mailto:cloudsupport@enterprisedb.com) including all necessary information for EDB to validate the claim.

To be eligible for a Service Credit you must:

Submit a support ticket with the Support Team within twenty-four (24) hours of becoming aware of an event that impacts service availability.

Submit your claim for a Service Credit within sixty (60) days of the event that impacted service availability.

Include all information necessary to validate your Service Credit request within your claim, including (i) a detailed description of the events resulting in Downtime, including your logs that document errors and corroborate the claimed outage, with confidential information redacted; (ii) the time and duration of Downtime; (iii) the number and locations of affected users as applicable; (iv) details regarding your attempts to resolve the Downtime at the time it occurred.

Reasonably assist the Support Team in investigating the cause of Downtime to process your claim.

Comply EDB documentation and guidance from the EDB Support Team.

In the event that the EDB Postgres Cloud Service does not meet the 99.995% Uptime availability, you may receive a Service Credit as set forth below:

SLA for PGD Clusters with Data Groups in Multiple Regions

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.995% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

SLA for HA Clusters and PGD Clusters with Data Group(s) in a Single Region

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

SLA for Single Node Clusters and Faraway Replicas

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.5% but equal to or greater than 99.0%	10%

Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

Service Credits are your sole remedy for any performance or availability issues and only apply to fees paid for the Cluster(s) or Faraway Replica(s) impacted for which a Service Level was not met. Service Credits are for future use of service and are capped at 100% of paid fees in the month in question.

Limitations

You will not be eligible for a Service Credit for any performance or availability issue that results from:

Factors outside of our reasonable control, such as natural disaster, war, acts of terrorism, riots, government action, or a network or device failure between your client application and EDB Postgres Cloud Service;

Services, hardware, or software provided by a third party, such as cloud platform services on which EDB Postgres AI runs;

Use of your password or equipment to access the EDB Postgres AI network;

Your or any third party's (a) improper use, scaling or configuration of EDB Postgres AI, or (b) failure to follow appropriate security practices; or

Your or any third party's tampering with cloud platform services, hardware, or software managed by EDB Postgres AI; or

Periods during which EDB Postgres AI has scheduled maintenance; or

EDB Postgres AI Beta or Tech Preview Offerings.

EnterpriseDB DataProcessing Addendum

Updated: October 2, 2024

1. Scope, Order of Precedence and Parties

This Data Processing Addendum ("DPA") applies to the Processing of Personal Data by EnterpriseDB Corporation and its Affiliates on Your behalf when providing Our Software, Cloud Services, Support Services or Professional Services ("Products and Services"). The Products and Services are described in the relevant license and/or services agreement and the applicable order (collectively, the "Agreement"). In the *event* of a conflict between the terms of the Agreement and this DPA, the terms of this DPA shall control. In the *event* of a conflict between the terms of this DPA and the EU Standard Contractual Clauses, the UK SEC Addendum, or Swiss Addendum (if applicable), the terms of the EU Standard Contractual Clauses, the UK SEC Addendum, Swiss Addendum or CCPA Addendum (if applicable) shall control.

This DPA is between the end-user customer ("You" or "Your") and the EnterpriseDB contracting entity ("EDB", "We", "Us" or "Our") and is incorporated by reference into the Agreement.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

2. Definitions

"Affiliate" means any subsidiary of EnterpriseDB Corporation that may assist in the processing of Your Personal Data under the Agreement and this DPA.

"Aggregate" means information that relates to a group or category of individuals, from which identities have been removed such that the information is not linked or reasonably linkable to any individual.

"Applicable Data Protection Laws" means (i) the EU General Data Protection Regulation 2016/679 ("GDPR") and laws or regulations implementing or supplementing the GDPR; and (ii) any other international, federal, state, provincial and local privacy or data protection laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective that apply to the Processing of Personal Data under the Agreement.

"Controller" is a legally defined term that generally refers to the party that determines the purposes and means (the why and how) of the processing of Personal Data.

"Personal Data" means any of your data uploaded, transmitted or otherwise Processed in connection with the performance of Products and Services that can identify a unique individual, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of individuals, or as otherwise defined under Applicable Data Protection Laws.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Us in order to perform the Products and Services.

"Processor" is a legally defined term that generally refers to the party that processes Personal Data on behalf of the Controller.

"Sub-Processor" means any third party engaged by a Processor or another Sub-Processor to assist with the Processing of Personal Data for the performance of Products and/or Services under the Agreement.

"Swiss SCC Addendum" means the adaptation of the 2021 EU SCCs designed to ensure an adequate level of protection for data transfers

from Switzerland to a third country subject to the Swiss Federal Act on Data Protection ("FADP").

"Usage Data" means technical data collected from Your use of Services for the purposes specified herein.

"UK Data Protection Laws" means the UK GDPR and the Data Protection Act 2018, or any successor UK data protection laws as updated, amended or replaced from time to time.

"UK SCC Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) (vB1.0 or any subsequent version) issued by the UK Information Commissioner's Office.

"2021 EU Standard Contractual Clauses" or **"2021 EU SCCs"** means the contractual clauses annexed to the EU Commission Decision 2021/914/EU (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) or any successor clauses approved by the EU Commission.

Terms used but not defined in this DPA (e.g., "Business Purpose", "Consumer", "Controller", "Data Subject", "Process/Processing", "Processor") shall have the same meaning as set forth in the Agreement or Applicable Data Protection Laws.

3. Roles as Controller and Processor

For purposes of this DPA, You are the Controller of the Personal Data Processed by EDB under the terms of the Agreement. You are responsible for complying with your obligations as a Controller under Applicable Data Protection Laws governing your provision of Personal Data to Us for the performance of the Products and Services, including without limitation obtaining any consents, providing any notices, otherwise establishing the required legal basis, and responding promptly to any inquiries from a data protection authority. Unless specified in the Agreement, You will not provide Us access to any Personal Data that imposes specific data protection requirements greater than those agreed to in the Agreement and this DPA, and you will limit Our access to Personal Data as necessary for Your use of the Products and Services under the Agreement.

EDB is the Processor and service provider with respect to such Personal Data, except when You act as a Processor of Personal Data, in which case We are a Sub-Processor.

EDB is responsible for the Processing of Usage Data solely for Our legitimate business interests, including, securing, managing, measuring and improving Customer's use of EDB Services in accordance with the Agreement and pursuant to the terms of this DPA.

Each party shall comply with their respective obligations as Controllers and Processors under Applicable Data Protection Laws.

4. EDB's Purpose of Processing

EDB and any persons acting under its authority under this DPA, including Sub-Processors and Affiliates as described in Section 7, will Process Personal Data only for the purposes of performing the Services in accordance with your written instructions as specified in the Agreement, this DPA, and Applicable Data Protection Laws. We may also Aggregate Personal Data as part of the Products and Services in order to provide, secure, and enhance EDB Services.

We will not disclose Personal Data in response to a subpoena, judicial or administrative order, or other binding instrument (a "Demand") unless required by law. We will promptly notify You of any Demand unless prohibited by law and provide You reasonable assistance to facilitate Your timely response to the Demand. We may provide Personal Data to Affiliates in connection with any anticipated or actual merger, acquisition, sale, bankruptcy, or other reorganization of some or all of its business, subject to the obligation to protect Personal Data consistent with the terms of this DPA.

5. CCPA Compliance

EDB will not process, retain, use, or disclose Your Personal Data for any purpose other than for the purposes set out in the Agreement, DPA and as permitted under the CCPA, where applicable. EDB will not Sell or Share Your information as those terms are defined under the CCPA.

6. Data Subjects and Categories of Personal Data

You determine the Personal Data to which You provide Us access to in order to perform the Products and Services. This may involve the Processing of Personal Data of the following categories of Your Data Subjects:

Employees and applicants

Customers and end users

Suppliers, agents, and contractors

The Processing of Your Personal Data may also include the following categories of Personal Data:

Direct identifiers such as first name, last name, date of birth, and home address

Communications data such as home telephone number, cell telephone number, email address, postal mail address, and fax number

Family and other personal circumstance information, such as age, date of birth, marital status, spouse or partner, and number and names of children

Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, and CV data

Other data such as financial, good or services purchased, and license details

Usage data including device and other identifiers, online profiles and behavior, and IP address

Other Personal Data to which You provide EDB access in connection with the provision of Services

7. Sub-Processing

Subject to the terms of this DPA, You authorize Us to engage Sub-Processors and Affiliates for the Processing of Personal Data. These Sub-Processors and Affiliates are bound by written agreements that require them to provide at least the level of data protection required of Us by the Agreement and this DPA, and We have implemented reasonable measures designed to confirm compliance with such measures. You may request Us to perform an audit on a Sub-Processor or to obtain an existing third-party audit report related to the Sub-Processor's operations to verify compliance with these requirements. You may also request copies of the data protection terms We have in place with any Sub-Processor or Affiliate involved in providing the Products and/or Services. We remain responsible at all times for such Sub-Processors' and Affiliates' compliance with the requirements of the Agreement, this DPA and Applicable Data Protection Laws.
A list of sub-Processors as well as a mechanism to obtain notice of any updates to the list, are available at https://trust.enterprisedb.com/subprocessors (https://trust.enterprisedb.com/subprocessors). At least thirty (30) calendar days before authorizing any new Sub-Processor to access Personal Data, We will notify you. Where EDB is a Processor, the following terms apply:

During this notice period, objections (if any) to EDB's appointment of the new Sub-Processor must be provided to EDB in writing and based on reasonable grounds. In such an event, the Parties will discuss those objections in good faith with a view to achieving resolution. If it can be reasonably demonstrated to EDB that the new Sub-processor is unable to Process YourPersonal Data in compliance with the terms of the DPA and EDB cannot provide an alternative Sub-Processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence, You, as Your sole and exclusive remedy, may terminate the Order Form(s) with respect to only those aspects which cannot be provided by EDB without the use of the new Sub-processor by providing advance written notice to EDB of such termination..
EDB will refund You any prepaid unused fees of such Order Form(s) following the effective date of such termination.
If the affected Product or Service is part of a suite (or similar single purchase of Products and Services), then any such termination will apply to the entire suite.

8. International Transfer of Personal Data

We may transfer Personal Data to the United States and/or to other third countries as necessary to perform the Products and/or Services, and you appoint EDB to perform any such transfer in order to process Personal Data as necessary to provide the Services. We will follow the requirements of this DPA regardless of where such Personal Data is stored or Processed.

Where the Processing involves the international transfer of Personal Data of a resident(s) of a country within the EEA, Switzerland or UK to EDB, Affiliates or Sub-Processors in a jurisdiction (i) that has not been deemed by the European Commission or the UK Information Commissioner's Office to provide an adequate level of data protection, and (ii) there is not another legal basis for the international transfer of such Personal Data, such transfers are subject to either the 2021 EU Standard Contractual Clauses, the UK SCC Addendum and/or Swiss SCC Addendum (as applicable) or other valid transfer mechanisms available under Applicable Data Protection Laws. For international transfers subject to:

the GDPR, the Parties hereby incorporate by reference the 2021 EU secs in unmodified form (Module One where You and EDB are both Controllers, Module Two where You are a Controller and EDB is a Processor, or Module Three where both You and EDB are both Processors, as applicable)

the UK Data Protection Laws, the Parties hereby incorporate by reference the UK sec Addendum in unmodified form

the FADP, the Parties hereby incorporate by reference the Swiss sec Addendum

The 2021 EU secs and the UK sec Addendum shall be between You and EnterpriseDB Corporation, irrespective of Your location. For such purposes, You will act as the Data Exporter on Your behalf and on behalf of any of Your entities, and EnterpriseDB Corporation will act as the Data Importer on its own behalf and/or on behalf of its Affiliates.

For each module of the 2021 EU secs, where applicable:

(i) Clause 7, any acceding entity shall enforce its rights through You;

(ii) Clause 9, option 2 ("General Written Authorization") is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 7 of this DPA;

(iii) Clause 11, the optional language of (a) will not apply;

(iv) Clause 17, option 1 shall apply and refer to the law of the Netherlands;

(v) Clause 18(b), disputes shall be resolved before the courts of the Netherlands;

(vi) Annex 1(A), purposes of processing, (B) categories of data subjects and personal data are specified in Section 6 of this DPA;

(vii) Annex 1(C) the data exporter's competent supervisory authority shall be determined in accordance with EU GDPR and Clause 13 of the Standard Contractual Clauses; and

(vii) Annex 2, technical and organizational security measures, are specified in Section 10 below.

For the purposes of the Swiss sec Addendum, (i) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the 2021 EU SCCs; (ii) the references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP; (iii) the Federal Data Protection and Information Commissioner of Switzerland shall be the competent supervisory authority in Annex I.C under Clause 13 of the 2021 EU SCCs, where the transfer of Personal Data is subject to the FADP.

In the event of any direct conflict between this Addendum and the 2021 EU Standard Contractual Clauses, the UK SCC Addendum and/or Swiss sec Addendum the 2021 EU Standard Contractual Clauses, the UK sec Addendum and/or the Swiss sec Addendum (as applicable) shall prevail.

9. Requests from Data Subjects

We will make available to You the Personal Data of Your Data Subjects and the ability to fulfill requests by Data Subjects to exercise one or more of their rights under Applicable Data Protection Laws in a manner consistent with Our role as a Processor. We will provide reasonable assistance to assist with Your response.

If We receive a request directly from Your Data Subject to exercise one or more of their rights under Applicable Data Protection Laws, We will direct the Data Subject to You unless prohibited by law.

10. Security

We shall implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Data against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such security practices are set forth in the EDB Information Security Exhibit located at https://trust.enterprisedb.com/securityexhibit (https://trust.enterprisedb.com/securityexhibit) at the time the services are performed. We seek to continually strengthen and improve its security practices, and so reserve the right to modify the controls described therein upon notice to you, either individually or via our website. Any modifications will not diminish the level of security during the relevant term of Services.

Our employees are bound by appropriate confidentiality agreements and required to comply with Our corporate privacy and security policies and procedures, including the applicable requirements of this DPA.

11. Personal Data Breach

We shall notify You without undue delay after becoming aware of a Personal Data Breach involving Personal Data in Our possession, custody or control. Such notification shall at least: (i) describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of Your Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) provide the name and contact details of a contact where more information can be obtained; and (iii) describe the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects. You will coordinate with Us on the content of any public statements or required notices to individuals and/or Supervisory Authorities.

12. Your Instructions and Providing Information & Assistance

You may provide additional instructions to Us related to the Processing of Personal Data that are necessary for You and EDB to comply with our respective obligations under Applicable Data Protection Laws as Controller and Processor. We will comply with such instructions, provided that in the event that Your instructionsimpose costs on Us beyond those included in the scope of Products and Services under the Agreement, the parties agree to negotiate in good faith to determine the additional costs. We will promptly inform You if We believe that Your instructions are not consistent with the Products and Services or Applicable Data Protection Laws, provided that We will not be obligated to independently inspect or verify Your Processing of Personal Data.

We will provide You information reasonably necessary to assist You in enabling Your compliance with Your obligations under Applicable Data Protection Laws as further specified in this DPA.

13. Return and Deletion of Personal Data

We will return or provide an opportunity for You to retrieve all Personal Data after the end of the provision of Services and delete existing copies. With respect to cloud services, You shall have thirty (30) calendar days to download Your Personal Data after termination of the Agreement and You must contact technical support for download access and instructions. In the event You do not contact technical support for this purpose within 30 calendar days after the end of the provision of Products and/or Services, We shall delete Your Personal Data promptly once that Personal Data is no longer accessible by You, except for (i) back-ups deleted in the ordinary course, and (ii) retention as required by applicable law. In the event of either (i) or (ii), We will continue to comply with the relevant provisions of this DPA until such data has been deleted. We will provide written confirmation of deletion upon request.

14. Audit

In the event the information you request of EDB under Section 12 above does not satisfy your obligations under Applicable Data Protection Laws, You may carry out an audit of Our Processing of Your Personal Data up to one time per year or as otherwise required by Applicable Data Protection Laws. To request an audit, you must provide Us a proposed detailed audit plan three weeks in advance, and We will work

with you in good faith to agree on a final written plan. Any such audit shall be conducted at Your own expense, during normal business hours, without disruption to Our business, and in accordance with Our security rules and requirements. Prior to any audit, We undertake to provide You reasonably requested information and associated evidence to satisfy Your audit obligations, and You undertake to review this information prior to undertaking any independent audit. If any of the requested scope of the audit is covered by an audit report issued to Us by a qualified third-party auditor within the prior twelve months, the parties agree that the scope of Your audit will be reduced accordingly.

You may use a third-party auditor with Our agreement, which will not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Us. If the third party is Your Supervisory Authority that applicable law enables it to audit Us directly, We will cooperate with and provide reasonable assistance to the Supervisory Authority in accordance with Applicable Data Protection Laws.

You will provide Us a copy of any final report unless prohibited by Applicable Data Protection Laws, will treat the report and findings as confidential information in accordance with the terms of the Agreement (or confidentiality agreement entered into between You and EDB), and use the report and findings solely for the purpose of assessing Our compliance with the terms of the Agreement, this DPA, and Applicable Data Protection Laws.

15. Term

This DPA becomes effective upon Your purchase of the Products and Services. Termination of the Agreement does not relieve either party of its obligations under this DPA.

Security at EDB

Version 2.0
Revised: 12/18/2024

Table of Contents

Table of Contents **2**
I. Security at EDB **3**
A. Oversight and Governance 3
B. Roles and Responsibilities 4
II. Program Overview **4**
A. Asset Management 4
B. Identity and Access Management 5
C. Change and Configuration Management 6
D. Data Management 6
E. Backup and Recovery 7
F. Business Continuity 7
G. Incident Response 7
III. Secure Operations **8**
A. Network Operations 8
B. Site Operations 8
C. Workplace Operations 9
D. Third Party Management 10
E. Vulnerability Management 11
IV. System Lifecycle and Monitoring **11**
A. System Lifecycle 11
B. System Monitoring 12
V. Training and Insider Threat **13**
Revision History **14**

This Security Standard describes the security controls of EnterpriseDB's ("EDB") cloud services, software products, technical support, and consulting services delivered to customers under the relevant agreement and the applicable order. Demos, betas or preview services, and internal IT systems not involved in the delivery of the Services described above are outside of the scope of this Security Standard.

I. Security at EDB

The EDB Security Standard describes the information security program implemented by EDB ("Information Security Program" or "Program"). The Program includes a comprehensive set of policies, procedures, and controls designed to protect the confidentiality, integrity, and availability of data and systems. The objective of the Program is to establish the ownership, accountability, and scope of EDB's information security activities. The Program aligns with applicable industry standards and best practices including but not limited to: ISO/IEC, PCI DSS, and Service Organization Controls (SOC).

A. Oversight and Governance

EDB has an established information security department with key stakeholders who are responsible for the development, implementation, and maintenance of the Program. EDB's Chief Information Security Officer (CISO) is responsible for oversight, policy strategy, compliance, and enforcement of EDB's Program.

EDB's program includes a formal cyber risk management function designed to identify and proactively respond to any potential threats to our products, services, or infrastructure. EDB's cyber risk program is managed by a security Steering Committee of cross-functional management and leadership personnel. The Steering Committee meets at least quarterly to provide oversight and guidance in identifying, assessing, and addressing security risk.

EDB's information security policies are reviewed and updated at least annually. The design and operating effectiveness of EDB's policies and internal controls are continuously evaluated, and corrective actions related to identified deficiencies are tracked to resolution.
EDB undergoes regular audits conducted by independent third parties. These audits assess the effectiveness of EDB's Program and identify any areas that need improvement.Details regarding EDB's external audits may be found in the EDB Trust Center.

B. Roles and Responsibilities

EDB believes that clear roles and responsibilities are essential for the protection of its data and systems. Roles and responsibilities within the Information Security Program are as follows:

Executive Leadership

- Support the Program by reinforcing the CISO's mission and executing decision-making authority to drive program goals, objectives, and priorities.
- Maintain an understanding of enterprise risks related to security.

Chief Information Security Officer (CISO)

- Provides oversight of the Program, including planning and implementation management.
- Oversees and approves information security policies necessary to identify and successfully manage and mitigate security risks.
- Manages the identification, implementation, and assessment of common security controls.
- Assists senior company officials across the company with their responsibilities for securing EDB.

CISO Staff

- Support the goals of the Program as requested by the CISO.

EDB Employees

- Understand, acknowledge, and adhere to EDB security policies.
- Implement the necessary processes and procedures to support established policies and controls.
- Identify, report, and seek guidance from management and/or the CISO on actual or suspected deviations from established policies and controls.

II. Program Overview

A. Asset Management

EDB maintains a comprehensive asset inventory that includes all assets, both on-premises and in the cloud. Assets are tracked and managed using unique identifiers and have designated owners. Discovery systems are in place to identify new assets as they are introduced into the environment. EDB's asset inventory is reviewed at least annually.

Formal data retention and disposal procedures are documented to guide the secure disposal and destruction of company, personnel, and customer data according to requisite compliance standards.

EDB's data center assets are protected by subservice organizations and their security practices. Security criteria are periodically evaluated and include asset management measures such as:

- Recording and authorizing the entry and exit of media at data center locations;
- Ensuring sensitive physical media is packaged securely and transported in a secure, traceable manner; and
- Prohibiting the use of portable media in datacenters unless explicitly authorized by IT or information security management.

These asset management measures help to protect EDB's data center assets from unauthorized access, use, disclosure, disruption, or destruction.

B. Identity and Access Management

EDB implements a comprehensive identity and access management policy ("IAM") that includes strong passwords, multi-factor authentication, password managers, privileged access controls, single sign-on, unique identifiers, access reviews, shared and group account restrictions, role-based logical access conforming to the "least privileges" standard, remote access restrictions, conditional authorization, end-user authentication, key management, and key storage and distribution. Controls include but are not limited to:

- EDB adheres to industry standards for its password complexity, rotation, and lockout policies.The use of multi-factor authentication is required for all enterprise access, remote sessions and access to environments that host production systems.
- Privileged logical access to production environments is enabled through an authorized session manager; session user activity is recorded and tunneling to untrusted data environments is restricted.
- Employees, contractors, and other corporate user accounts use single sign-on (SSO) for enterprise systems.
- Access groups used in provisioning entitlements for an account are defined, with owners, and are reviewed on a regular basis. Group owners are responsible for approving access to authorized individuals.
- EDB conducts periodic access reviews by managers for the in-scope system components to ensure that access is restricted appropriately, and corrective action is taken where applicable.
- Where applicable, processes that run as part of an EDB shared hosting platform will run under unique credentials that permit access to only one customer environment.

C. Change and Configuration Management

EDB has established a process to address the lifecycle of technology change practices, including communication for maintenance and downtime. The process addresses security requirements and requires that software and infrastructure changes be authorized, formally documented, tested (as applicable), reviewed, and approved prior to deployment to production environment(s).

Infrastructure and software changes are managed and tracked using work management systems. To ensure separation of duties is maintained, the process is appropriately segregated and access to migrate or approve changes is restricted to authorized personnel.

EDB implements the following configuration management policies and processes to ensure and maintain the integrity of its systems:

- Secure baselines are established for key assets in accordance with industry standards.
- Unauthorized changes to EDB's configuration management policies are tracked and actioned in a timely manner.

D. Data Management

EDB commits to protect the confidentiality, integrity, and availability of all data entrusted to it, including EDB data and client data. EDB will implement appropriate security measures to protect data from unauthorized access, use, disclosure, disruption, or destruction. These measures include:

- Classifying data according to its sensitivity and implementing appropriate security controls for each classification level.
- The use of industry standard encryption algorithms to project confidential data at rest and in transit.
- Regularly review encryption practices to ensure that they remain effective.
- Redacting or otherwise sanitizing confidential data prior to use in a non-production environment(s).
- Disposing of data securely in accordance with applicable laws, regulations, and contractual requirements.

EDB regularly reviews and updates its security measures to ensure that they remain effective in protecting data. EDB will also provide ongoing training to personnel on data security best practices.

E. Backup and Recovery

EDB maintains a comprehensive backup and recovery plan that includes daily incremental and weekly full backups of all data stores housing sensitive customer data. Backups are encrypted and securely stored in an alternate location from the source data. EDB periodically tests the backup restoration to confirm the reliability, functionality and integrity of system backups or recovery operations, at least annually.

Business continuity and disaster recovery plans are reviewed annually, or when necessitated by system or business changes and approved by management.

F. Business Continuity

EDB strategically plans for the continuity of business operations if adverse or potentially disruptive events impact business operations. EDB maintains a comprehensive business continuity plan that includes a periodic business impact analysis to identify relevant threats to assets, infrastructure, and resources that support critical business functions. The business continuity plan is reviewed and approved by management and communicated to relevant team members at least annually. At a minimum, EDB's business continuity plan includes:

- Recovery objectives for critical business functions.
- Detailed disaster recovery protocols, designed to enable the operational recovery of systems.
- Defined recovery scenarios, including recovery point objectives (RPO) and recovery time objectives (RTO).
- Business contingency roles, responsibilities, and contact information, which are assigned to individuals and communicated to authorized personnel.
- Processes and requirements for business continuity plan testing performed at least annually.

G. Incident Response

EDB has a comprehensive incident response (“IR”) policy that includes an IR Plan, processes, and training. Additionally, criteria are defined for reporting requirements, response testing, and postmortem analysis. The controls include but are not limited to:

- An IR Plan that defines the types of incidents to be managed, tracked, and reported, and procedures to manage incidents through the lifecycle.
- Prioritization and escalation of confirmed incidents to ensure management to resolution. If applicable, incident response with business contingency activities is executed.

- EDB trains First Responders annually through Incident Response training, covering best practices for evaluating events, classifying incidents, and IR procedure engagement.
- Incident Response processes are tested at least annually. Results from these tests are documented and remediations prioritized.
- EDB external communication requirements are defined by type of incident, mitigations required, and possible impact to external parties including notifications.
- EDB takes its data breach notification obligations seriously and maintains a "customer protection first" approach, committing to expedited notification in the event customer impact is determined.

III. Secure Operations

A. Network Operations

EDB implements a comprehensive network operations program that includes network segmentation, perimeter security, ingress and egress point hardening/monitoring, firewalls and other security controls which include but are not restricted to:

- Logical segregation of production environments based on defined and established criteria.
- The deployment of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) across critical infrastructure for continuous monitoring.
- Monitoring and protecting critical services from Denial of Service (DoS) attacks.
- The use of a managed dynamic blocklist to deny malicious network communications across the enterprise.
- Dynamic packet filtering enabled on the network.
- Network firewall rule sets are reviewed on at least an annual basis or as required in response to major changes in the environment.
- Network ingress and egress points are inventoried; this inventory is reviewed annually.
- Inbound and outbound network traffic with untrusted networks passes through a policy enforcement point or firewall.

B. Site Operations

Please note that this section addresses the physical and environmental security requirements for accessing data center locations that are not cloud based.

EDB is committed to protecting its technology systems from unauthorized access, damage, or destruction. To help ensure the security of its systems, EDB has physical and environmental security policies in place. These policies apply to EDB corporate offices and are levied as requirements on any third-party facilities or Cloud Service Provider (CSP) hosting EDB workloads. The following list, while not exhaustive, outlines some key elements of EDB's physical and environmental security requirements:

- CSPs employ physical access control mechanisms to restrict access to only authorized personnel and third parties. These controls are designed to comply with all applicable regulations, including health and safety regulations, building codes, and fire prevention codes.
- The provision and modification of permissions associated with physical access roles are approved by authorized personnel. Physical access that is revoked when no longer required.
- Access to CSP or datacenter facilities requires management approval and documented requirements before access is granted.
- CSPs deploy intrusion detection and video surveillance systems at data center locations; confirmed incidents are documented and tracked to resolution.
- CSP ensures physical access points to server locations are protected by video surveillance and footage is retained for 90 days, unless limited by legal or contractual obligations.
- Access records to the facility are retained for a minimum of 365 days.
- Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks. Power and telecommunication lines are protected from interference, interception, and damage.
- Uninterruptible power supply (UPS) and generators are employed to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified as required.
- Temperature and humidity levels of data center environments are monitored and maintained at appropriate levels.

C. Workplace Operations

EDB manages all enterprise devices to ensure that they are compliant with the organization's security policies. This includes but is not limited to:

- Enrolling all enterprise devices in device management.
- Maintaining an inventory of all enterprise devices and software.
- Installing endpoint security on all enterprise devices.
- Encrypting storage installed on all enterprise devices.

EDB has a defined and published enterprise device baseline that outlines the requirements for managed and trusted devices. Enterprise managed devices are

required for access to critical systems. Devices, applications, and software are cataloged in an inventory that is updated at a minimum annually and in accordance with appropriate security standards.

Baselines are in place and are reviewed at minimum annually or as required. Minimum requirements include:

- Devices are configured to ensure unnecessary hardware capabilities and functionalities are disabled.
- Screen lock requirements are in place.
- Users are locked out of information systems after a defined number of unsuccessful consecutive attempts.
- Accounts remain locked for a defined period or until an administrator enables the user ID.

D. Third Party Management

EDB may use vendors, third parties, and contracted resources to support its services and operations. Procurement, legal and security teams perform due diligence reviews of any vendor with access to EDB's data, networks, or systems, and for any vendor providing critical product and infrastructure services. Analysis and acceptance of vendors are managed within tiers based on their criticality to the organization and its operations.

EDB enters into contractual agreements with vendors who process or store data; information security terms and service level agreements are defined as part of that contractual relationship. For critical vendors, these agreements will include a Vendor Information Security Addendum that defines the responsibilities and governance requirements regarding information shared during vendor engagements.

EDB has established processes to request and review vendor provided attestation reports or vendor risk assessments to ensure the vendor maintains the standards of the agreed upon posture. For critical vendors, these reviews are performed on an annual basis. This will be requested for all critical vendors to ensure the evaluations and impact of noted exceptions of service.

EDB performs a risk assessment review to determine the data types and access that can be shared with a vendor. If material risks are identified with any vendor, EDB will attempt to mitigate the risk in accordance with internal remediation policies and strategies.

EDB maintains a list of third-party vendors and approved relationships. This list is reviewed, and updated on a periodic basis. All EDB vendors who hold critical data and who have network access are proactively reviewed and continuously monitored.

E. Vulnerability Management

EDB has an established framework for reviewing, evaluating, and verifying malware protection, conducting penetration testing and production scanning of the environment and infrastructure. This includes the remediation timelines for triaged vulnerabilities.

EDB monitors applications, systems, and environments for vulnerabilities on a regular cadence with automated vulnerability scanners. Additionally, EDB has an established penetration testing function which periodically conducts tailored pen-tests against production environments.

Any identified findings or vulnerabilities are required to be remediated within established timelines. Remediation timelines align to industry standards and best practices:

- Critical Severity - triaged within 72 hours and addressed within 14 days.
- High Severity - addressed within 30 days.
- Medium Severity - addressed within 90 days.
- Low Severity - addressed within 150 days or best effort unless tied to risk mitigation.

In the event a patch, update, or permanent mitigation is not available, appropriate countermeasures will be used to reduce the risk of exploitation of the vulnerability. This process is formally documented via a vulnerability deferral program which is used to track deferrals into future remediation.

Secure configuration baselines are in place and are reviewed on an annual basis, or as needed.

IV. System Lifecycle and Monitoring

A. System Lifecycle

EDB is committed to protecting its technology systems from unauthorized access, damage, or destruction. To help ensure the security of its systems, EDB has made commitments to manage capacity, firmware, patch, and code release practices.

EDB follows a formal systems lifecycle methodology to govern the development, acquisition, implementation of changes, and maintenance of information systems, software, and related technology requirements. This includes adequately transitioning End of Life (EoL) and/or End of Support (EoS) software, systems, or technologies.

EDB has an established Application Security program to define security controls and processes to be used by developers within the organization. This includes managing source code with approved version control mechanisms, and ensuring code deployments are reviewed and approved by an authorized manager or designated process owner. As part of the development pipeline, EDB checks source code for vulnerabilities, including code injection, buffer overflows, insecure cryptographic storage, insecure communication, improper error handling, high-risk vulnerabilities, cross-site scripting, improper access control, cross-site request forgery, and broken authentication session management.

EDB manages and installs security-relevant patches for operating systems, prioritized by the criticality of vulnerabilities addressed. Absent exceptional circumstances, EDB operates under the following resolution timelines:

- Critical Severity - triaged within 72 hours and addressed within 14 days.
- High Severity - addressed within 30 days.
- Medium Severity - addressed within 90 days.
- Low Severity - addressed within 150 days or best effort unless tied to risk mitigation.

B. System Monitoring

EDB collects and uses logs for providing, securing, managing, measuring, and improving its ability to troubleshoot system issues, identifying security events, and protecting and securing its networks and products. Logs may also be collected for compliance with agreements, policies, and legal or regulatory requirements. Logging may include monitoring the performance, stability, usage and security of services and related components along with defined critical information system activity.

EDB defines security monitoring alert criteria that includes (but is not limited to) the following parameters:

- Monitoring all individual user access with root or administrative privileges.
- Invalid logical access attempts.
- Limit viewing of logs by authorized personnel.
- Monitoring of activities based on system log in.
- Individual authorized user access attempts.
- Reports on audit logs ‘cleared.’

An established process exists for flagging alerts, and for sending confirmed alerts to authorized personnel for triage and response.

V. Training and Insider Threat

EDB requires all new hires and contractors to pass a background check as a condition of employment. Candidates are interviewed to assess, among other things, insider threat risk. All new EDB personnel complete HR and IT onboarding, which includes a requirement to assent to all key company policies.

In addition, EDB has established an ongoing training and awareness program to ensure that all EDB personnel, contractors and clients who use EDB systems and data are aware of their responsibility to safeguard EDB internal and confidential data.

- All EDB personnel and contractors must complete a Security Awareness training at onboarding and at minimum refresh their training annually. Training includes EDB policies, and how to report security events to the authorized response team.
- Personnel with key security responsibilities complete relevant role-based training on an annual basis.
- EDB's software engineers are required to complete training based on their role. Training content varies between industry relevant secure coding techniques and best practices.

Revision History

Version	Summary of Changes	Name	Date
1.0	Initial Draft	Dani Shepard	06/5/2024
2.0	Revised to align with current branding and procedures	Sara Gaylord	12/18/2024


EDB