Cybersecurity Exhibit - For Purchase Orders for Subscription or Software as a Service

Revision date: 07/01/2025

This Cybersecurity Exhibit ("**Exhibit**") is incorporated into and forms a part of the Purchase Order. The terms of this Exhibit shall apply to and be binding upon the Provider and the Provider's performance of Services to the extent applicable to such Services and are in addition to any terms regarding cybersecurity contained in the Purchase Order.

1. Definitions

When used in this Exhibit, the following defined term shall have the meaning shown below:

"Agreement" shall mean a Purchase Order, between Client and Provider, for the performance of Services or which establishes terms and conditions for the performance of Services and to which this Exhibit is appended or into which this Exhibit is incorporated

"Backups" means backups containing copies of all Client Data residing on Provider's Systems.

"Client" means ConocoPhillips Company or its affiliate (as applicable) receiving the Services pursuant to the Agreement.

"Client Data" means any and all materials, information or data owned, controlled, or maintained by or concerning Client or its assets or its employees or personnel, including, but not limited to, any technology, intellectual property, data, information or material provided or submitted by or on behalf of Client to Provider or its system or application in connection with the performance of Services, including Personal Data. For clarity, Client Data shall include Personal Data of Client and its employees, representatives, customers, and others with whom Client does business which is received by, made available to, or accessed by or on behalf of Provider in connection with the Agreement.

"Data Protection Laws" means any applicable current or new laws, regulations, governmental requirements, and industry standards applicable to Provider's processing of Client Data, as they may be amended or updated from time to time, including, but not limited to, the General Data Protection Regulations ("GDPR") as defined under European Regulation 2016/679, the California Consumer Privacy Act of 2018 ("CCPA"), the California Privacy Rights Act ("CPRA"), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Data Protection Act, and any other applicable state, national, provincial or federal law of similar import or which address similar subjects.

"Personal Data" means data or information, in any form or format, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, consumer, or household, including any derivatives thereof or inferences made therefrom, and any other information that is regulated as "personal data", "personally identifiable information", "personal information", or similar terms under Data Protection Laws.

"Provider" means the person or entity providing or performing Services to Client pursuant to the Agreement.

"Provider Personnel" means the employees, officers, independent contractors, and individual agents of the Provider and Provider Third Parties.

"Provider Security Program" means a current and comprehensive data security program which includes reasonable and appropriate administrative, technical, and physical safeguards and organizational security measures.

"Provider Systems" means computing equipment, systems, applications, and software used by or for Provider to access, receive, generate, handle, store, transmit, or otherwise process any Client Data.

"Provider Third Parties" means Provider's subcontractors, subprocessors, contractors, and agents.

"Security Incident" means any actual or suspected alteration, disclosure or loss of, or inability to access or account for or recover, or any incident relating to unauthorized access to, use, disclosure, modification, processing, destruction, or acquisition of, any or all of Provider's computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system owned or controlled by Provider or Provider Third Parties, or networks, physical or virtual infrastructure controlled by computers or information systems, as well as any event that involves the security of Provider Systems or its supply chain, and applicable services. This "Security Incident" definition includes an event that is under investigation or evaluation without final determination of the event's root cause.

"Services" means providing or performing services or work, storing, manipulating, or processing data or information, or permitting, authorizing, or licensing access to and/or use of databases, applications or tools, as set forth in the applicable Agreement.

2. Security & Backup

2.1 Identification of Personnel with Access. Provider shall identify to Client all Provider Third Parties who will have access to Client Data in connection with performance of the Services. Provider will bear its own costs for such identification effort. Provider must obtain Client's written approval prior to such Provider Third Parties accessing or receiving Client Data, which approval shall not be unreasonably withheld. Only Provider and Provider Third Parties approved by Client are to be permitted access to Client Data, and Provider shall not permit access to such information by any other person. To the extent a Provider Third Party is identified as having access to Client Data in the Agreement, such Provider Third Provider shall be deemed approved by Client.

2.2 Personnel Vetting and Background Checks. All Provider Personnel performing hereunder may be subject to a background check by Client, at Client's sole discretion. Provider hereby consents to any such background checks and shall cause Provider Third Parties to consent to such background checks. Provider agrees that it will perform its own background checks, including but not limited to, fingerprint checks by appropriate law enforcement, verification of employment, and criminal background checks going back seven (7) years, on all Provider Personnel who are intended to have access to Client Data. Provider shall have a continuing duty to notify Client of any convictions involving theft, dishonesty, violence, breach of trust, money laundering, the illegal manufacture, sale, distribution of, or trafficking in controlled substances involving any such Provider Personnel having access to Client Data throughout the period that person has such access.

2.3 Provider Security Program. Provider shall implement and maintain a Provider Security Program with respect to all business processes and physical premises and all Provider Systems, to protect against any Security Incident.

2.4 Disaster Recovery Program. Provider warrants that it has established and shall maintain reasonable and appropriate disaster recovery measures designed to promptly restore Services and ensure their continuous and uninterrupted availability. Provider shall ensure that its procedures and measures provide for any period of unavailability of the Provider Systems and Services to Client after a failure or disaster to be no longer than 24

hours (unless another period is specifically provided in the applicable Agreement or in an applicable Service Level Agreement or similar document incorporated therein ("SLA")).

2.5 Backups. Provider shall maintain Backups on magnetic or other media in accordance with industry standards. At Client's request, Provider shall provide Client with copies of the Backups at such intervals, in such quantities, and in such format as Client may reasonably request. Provider shall maintain the Backups to ensure that Provider can restore the Provider Systems and Services such that, upon a recovery from a failure or disaster, the Client Data will be restored to a point no more than 24 hours before the failure or disaster. Provider shall ensure that processing can be properly resumed in the event of failures, which include mechanical, electronic, or communication failure.

2.6 Provider Third Parties. Before granting access to Client Data, Provider shall ensure that Provider Third Parties maintain data security programs which address the same requirements as the Provider Security Program and which are at least as protective as the Provider Security Program. The Provider Security Program, as well as security programs of Provider Third Parties, shall be in accordance, in structure and operation, with generally accepted industry standards and practices and, at a minimum, are to include those standards set forth in this Exhibit. Provider shall be responsible for the acts and omissions of all Provider Third Parties under the Agreement and this Exhibit as though such acts or omissions were those of Provider. Provider shall be responsible for ensuring that all Provider Personnel comply with applicable Data Protection Laws and will require Provider Personnel to complete adequate training regarding applicable Data Protection Laws. Provider specifically acknowledges and agrees that it will provide appropriate security to protect against unauthorized access by "insiders" (i.e., persons who have been given access to Client Data or systems containing Client Data in order to perform computer related services, but who may intentionally or inadvertently cause damage to data or to the system). "Insiders" shall be deemed to include, but shall not be limited to, current and former Provider Personnel.

2.7 Data Security Program Documentation. The content and implementation of the Provider Security Program shall be fully documented in writing by Provider, and Provider shall provide, or cause to be provided, comprehensive training to all of its employees on Provider's Security Program. Similarly, Provider shall obtain documentation of the content and implementation of Provider Third Parties' data security programs or obtain independent security reports (e.g., SOC2 Type II) that are acceptable to Client. Data security program documentation shall include control architecture, encryption, and data separation procedures, access control and verification, the presence or absence of audit trails, system testing and monitoring, disaster recovery and back-up, and program responsibility. Provider shall permit Client to review such documentation and to verify Provider's compliance with such program. Provider shall update in writing the information required by this Article upon the earlier of a material change or at least once every twelve (12) months.

2.8 Audit. Provider will provide a copy of the most recent SOC2 report and/or active ISO27001 certificate (or similar audit report acceptable to Client) to Client upon request, but no more than once a year. Upon Client's request, Provider shall provide evidence confirming the ongoing data privacy and cyber security compliance requirements. Provider shall disclose to Client any security breaches or incidents which may have involved the compromise of confidential information, sensitive data, or security controls. Within ten business (10) days after receipt of written notice from Client, Provider will provide Client and its external auditors with access (and will obtain access from Provider Third Parties) to applicable systems, records, certifications and supporting documentation as may be required by Client to enable Client to audit Provider's compliance with its information security obligations under this Exhibit. Provider will respond promptly to all security audit, discovery, and testing requests from Client and will cooperate with Client as required.

2.9 Material Changes. Provider shall notify Client in advance of any material changes being made to the way the Services are delivered to Client. "Material changes" shall include, without limitation:

a. relocation of the technical infrastructure, processing, or storage to a different data center, cloud provider, or jurisdiction;

b. addition of a new Provider Third Party that will have access to Client Data; and

c. any other change which Provider believes or should reasonably believe might alter or weaken the security of Client Data.

2.10 Return/Destruction of Client Data. Whenever Client Data is no longer needed for the performance of Services, or at any time upon written notification from Client, Provider shall unconditionally and without any charge or fee return or, at Client's written election, securely destroy any or all Client Data in Provider's custody or control (including Client Data in the custody or control of any Provider Third Parties) save and except for any Client Data as to which return or destruction is not technically feasible or legally permitted and which will be protected as required in this Exhibit and securely destroyed in the normal course of Provider's record retention program.

2.11 Storage Medium. To the extent Provider removes Client Data from any electronic medium under its control that is retired or taken out of service, Provider shall permanently destroy or securely erase Client Data through either: (i) physical destruction of the media; or (ii) erasure through one-pass, forensic-standard, overwrite of every byte on the disk, including slack space. Under no circumstances shall Provider use or re-use, for any purpose, electronic media on which Client Data has been stored unless Client Data has been securely and permanently erased in the manner described above. In addition, all Provider laptop hard drives on which Client Data may be stored are to be encrypted with up-to-date, industry standard encryption methods. Provider shall monitor use of any other media on which Client Data may be stored and shall utilize any improved data destruction methodologies on any such other media as such methodologies are implemented by Provider.

2.12 Separation of Client Data. Where physical separation of Client Data is not possible, Provider shall provide logical separation of Client Data from data of other organizations when storing the Client Data in databases, hard disks, backup/ archive media, or in information systems in Provider's alternative facilities (e.g., hot/ warm or cold sites).

2.13 Physical Security. Provider shall ensure that its facility is restricted to authorized personnel and that physical security controls are in place to deter, delay, detect, and deny physical access and to protect the security, confidentiality, privacy, integrity and availability of the Services. Access to Client Data that is identified by Client as "Restricted Confidential" shall require two-factor identification. If Provider is performing Services at Client's facility, Provider's personnel shall adhere to Client's physical security standards to achieve the physical security requirements.

3. Access Management; Password Authentication

3.1 Prevention of Unauthorized Access. Provider shall restrict and maintain security control to prevent unauthorized access to Client Data or Provider's systems or property, except by Provider Personnel who have been approved in accordance with the requirements of this Exhibit and who have a business need to access the Client Data and the Provider Systems to perform a particular function related to the Services. Provider shall notify Client as soon as possible, but in any event within 24 hours, when remote or onsite access to Client's Data or Client's premises should no longer be granted to particular Provider Personnel or Provider Third Parties.

3.2 Access Control Mechanism. If Provider provides mechanisms to allow Client to manage and control access, the provided functionality must be secure and protected from unauthorized access. The mechanisms for controlling access must be tested and shared in easily trainable format with Client prior to commencement of Services.

3.3 User Credentials. Provider shall provide user access using unique user credentials rather than only generic username and password. Provider shall allow Client users to change Provider-furnished passwords to their own unique passwords.

3.4 Audit Logging. Provider shall maintain, and provide to Client upon request, audit logging a minimum of 90 days of user activity throughout the identity and access management lifecycle (e.g., session logon, logoff, lock, failed logon attempts, accurate date/time stamps, actions performed, non-repudiation, etc.).

3.5 Authentication. Where password authentication is used in Provider's systems or Services, Provider shall ensure the following security features are enabled:

(a) Ability to enforce a minimum password length;

(b) Ability to set a password expiry date;

(c) Option for password complexity requirements;

(d) Ability to lock the account after a pre-defined number of failed logon attempts;

(e) Ability to prohibit the use of blank passwords;

(f) Provision of multi-factor authentication options for access to systems handling Client Data; and

(g) Ability to immediately lock the account of a terminated user.

Provider shall support Single Sign On Authentication and support IP Based restrictions to ensure access can be restricted to Client's network. Additionally, Provider shall support multi-factor authentication.

3.6 Remote Administrative Access. Provider shall utilize multi-factor authentication for all remote administrative access, including but not limited to access to Client's systems or networks and Provider Systems.

4. Data Breach; Security Incident

4.1 Security Incident Procedure. The Provider Security Program must include documented procedures to respond to any Security Incident and appropriate technical and procedural mechanisms for detecting, logging, analyzing and resolving unauthorized attempts to access the Client Data.

4.2 Designated Point of Contact. Provider shall appoint a designated point of contact ("POC") who will act as the primary liaison for all Security Incidents. Provider shall furnish the name and contact information to Client on the effective date of the Agreement. The POC shall coordinate and communicate relevant information related to all Security Incidents. Provider and Client shall conduct regular reviews on a mutually agreed schedule to confirm and, if necessary, update the designated POC throughout the term of the Agreement.

4.3 Security Incident Response. If Provider discovers or is notified or otherwise becomes aware of a breach or potential Security Incident that may affect the confidentiality, availability, or integrity of Client Data in the custody or control of Provider or of Provider Third Parties, Provider shall:

a. notify Client as soon as reasonably possible (and in any event no later than 48 hours after Provider discovers or is notified or otherwise becomes aware) of any Security Incident that may become known to Provider, Provider Personnel, or Provider Third Parties;

b. promptly furnish to Client full details of the unauthorized possession, use, or knowledge, or attempt to gain same, and assist Client in investigating and preventing the recurrence of any unauthorized possession, use of, or knowledge of Client Data, or attempt to gain same, through cooperation with any reasonable e-discovery and forensics processes required by Client. Such notification shall include, at a minimum and to the extent known following a reasonable inquiry carried out in accordance with the Provider's incident response procedures, information on (i) the extent and nature

of the Security Incident, (ii) the estimated risks and likely consequences of the Security Incident to each party, and (iii) the investigative, corrective, and remedial actions taken, planned, or proposed to prevent, contain, mitigate, and remediate the Security Incident;

c. as information becomes available, promptly furnish a detailed breakdown and description of the categories and volumes of affected Client Data and the Provider Systems and Client's systems or networks involved;

d. establish and maintain a weekly (or more frequent, as dictated by the situation) cadence for providing updates to Client regarding the Security Incident, the weekly updates to include written reports outlining the current status of the Security Incident investigation, actions taken (e.g. initiation of a forensic investigation), impact to Client Data, and any additional steps required for resolution;

e. cooperate with Client with respect to the investigation of third parties deemed necessary by Client to protect Client's proprietary rights and any subsequent litigation, to the extent such investigation or litigation relates to the Services; and

f. promptly take appropriate remediation measures to prevent a recurrence of any such unauthorized possession, use of, or knowledge of Client Data, or of any attempt to gain same and inform Client on an ongoing basis regarding same.

4.4 Confidential Information. Provider shall treat any Security Incident as confidential and to be shared only with Client and those personnel who have a business need-to-know. This includes any information once the Security Incident has been identified, information obtained during the incident resolution, and post-incident information communicated with Client.

4.5 Cooperation. Provider agrees to cooperate with Client and assist with any investigation-related requests, including, but not limited to, physical and logical access to the systems affected and facilitating communication with any individuals working for or on behalf of Provider or any other individuals who may be involved in or witness to the Security Incident until resolution to Client's satisfaction.

4.6 Records and Logs. Provider agrees to provide the relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, or industry standards, or as otherwise required by Client, and provide preventive measures to avoid reoccurrences.

4.7 Notice of Security Incidents. Subject to requirements of Data Protection Laws, Client will determine how, whether, and when to provide notice of a Security Incident affecting Client Data to (a) any companies or individuals whose information has been actually or potentially compromised; (b) any governmental authority; and/or (c) any other entity, including, but not limited to, consumer credit reporting agencies or the media. In addition to its obligations under applicable law, Contractor shall provide such notice of Security Incidents to affected persons if directed by Client. All notices and other public communications about any Security Incident must be approved by Client in writing before they are distributed or released.

4.8 Cost and Liability. Provider shall reimburse Client for costs, expenses and fees (including reasonable attorneys' fees) incurred by Client in connection with any such Security Incidents, including, but not limited to, costs involved in investigating such Security Incidents, costs involved in securing, preserving and regenerating Client Data, and fines and penalties arising out of such Security Incidents. In addition, if the Security Incident involved confidential or proprietary information of a third party for which Client may be liable or accountable pursuant to any contractual or legal theory, Provider shall reimburse Client for any costs, expenses, and fees incurred by Client in addressing or responding to third party claims and for any damages payable to such third parties.

4.9 Unavailability of Client Data. In addition, if the Security Incident involves unplanned unavailability of any Client Data as a result of any act or omission of Provider (including any act or omission of Provider Third Parties)

or damage to, impairment of, disablement of, or loss of use of any computer system, hardware, software, data, tangible property, then Provider shall reimburse Client for costs or expenses Client incurs in connection with containing, mitigating, and remediating such damage or unavailability, including but not limited to regeneration or replacement of any lost Client Data. Without limiting the foregoing, Client may take reasonable and appropriate steps to stop and remediate any unauthorized use of Client Data.

5. Compliance and Cooperation

In addition to the obligations set forth above in this Exhibit and the other provisions of this Agreement, the provisions which follow shall also apply to the extent applicable to the Services.

5.1 Adjustment of Policies. In the event of a difference between (a) Client's privacy, data security and/or records retention policies that Client makes known to Provider; (b) Provider's privacy, data security and/or record retention policies; and (iii) generally accepted industry standards and practices, Provider shall adjust its privacy, data security and/or records retention program to meet the policy or standard or practice that is more protective of Client Data. To the extent appropriate, the remuneration to Provider will be equitably adjusted to take account actual increased cost of performance.

5.2 Record Retention. If Client specifies retention periods in writing for any of the Personal Data or other Client Data that is maintained by Provider in connection with the Services, Provider shall maintain records containing such information for the corresponding period (subject to Client's rights under Article 2.10). In addition to the requirements above, Provider shall comply with all applicable laws concerning records retention that may apply to records used or created in connection with the Services and with any additional requirements applicable to Client's business that Client may provide to Provider and that may affect records retention for Client Data, including but not limited to e-discovery and legal hold orders.

5.3 Determination of Procedures. During the design, implementation, and setup, Client and Provider shall cooperate to determine the steps and procedures that would need to be implemented by Provider to comply with the obligations outlined in this Exhibit that are applicable to the Services and to document which of those steps and procedures are not already part of Provider's Services delivery plan as of the effective date of the Agreement. Provider shall implement the steps and procedures necessary for compliance with the obligations outlined above and that are approved by Client. To the extent appropriate, the remuneration to Provider will be adjusted to take account of any duly substantiated actual increased cost of performance, and other provisions of the Agreement will be adjusted as necessary.

5.4 Term. The requirements of this Exhibit shall remain in effect with respect to Client Data for so long as such Client Data remains in the custody or control of Provider or any Provider Third Party.