Terms of Use of Boeing Information and Electronic Systems

Rev. 02/2020

1. Definitions.

1.1. “Access Controls” is defined as procedures, mechanisms, and/or measures that limit access to Boeing Systems to authorized persons or applications.

1.2. “Boeing Systems” is defined as any electronic information systems operated by Buyer or operated by a third party on behalf of Buyer, including without limitation: facilities, network communications systems, telecommunications systems, software, applications, information and data.

1.3. "Contract" or “Agreement” used interchangeably means any Agreement between Seller and Buyer into which these Terms of Use of Boeing Electronic Systems Supplement are incorporated.

1.4. “Electronic Access” is defined as access by authorized Seller Personnel to the Boeing Systems with the ability or the means necessary to read, write, modify, or communicate information, or otherwise use authorized system resources.

1.5. “Malware” means malicious computer software that interferes with normal computer functions or causes information leakage to unauthorized parties.

1.6. "Materials" means all data, text, graphics, animation, audio and/or digital video components that are stored or hosted by Seller in relation to a Contract or that are accessible through Boeing Systems.

1.7. "Security Breach" means any suspected or actual compromise of an information system, including accidental or Unauthorized Use, disclosure, destruction, loss, alteration, transmission, or access to Buyer Materials that are stored or otherwise processed by Seller in relation to the Agreement.

1.8. “Seller Personnel” is defined as any of Seller's employees, contract labor, consultants, advisers, or other representatives who have a need to access the Boeing Systems for Seller to perform under this Contract.

1.9. “Seller Systems” is defined as any and all electronic information systems operated by Seller or operated by a third party on behalf of Seller, including without limitation: facilities, network communications systems, telecommunications systems, software, applications, information and data.

1.10. "Unauthorized Use" is defined as any use, reproduction, distribution, transfer, disposition, disclosure, possession, memory input, alteration, erasure, damage or other activity involving Materials, that is not expressly authorized under this Agreement (or any applicable Contract).

2. Access Right. Buyer grants to Seller a limited, nontransferable, nonexclusive, revocable (at Buyer’s discretion) right to access the Boeing Systems electronically solely during the term of this Contract and solely to the extent authorized in writing by Buyer in support of work to be performed by Seller pursuant to the Contract. Without limiting the foregoing, Seller hereby warrants that Seller and Seller Personnel shall not (i) introduce any Malware into Boeing Systems (whether through a laptop computer or other access device or otherwise); (ii) use the Boeing Systems for nonbusiness purposes including, without limitation, Unauthorized Use; and/or (iii) take actions calculated to disrupt Boeing Systems.

3. Privacy and Right to Monitor. Any communications or data transiting or stored on a Buyers Information System may be monitored, intercepted, recorded, and searched at any time and for any lawful purpose, and may be used or disclosed for any lawful purpose.

4. Electronic Access Requirements. Seller may request, and Buyer may provide in its sole discretion for Seller’s support of the Contract, Electronic Access for Seller Personnel on a "need to know" basis. When Electronic Access is provided to Seller, these Section 4 terms apply:

4.1. Accounts & Access Controls: Prior to obtaining Electronic Access, authorized Seller Personnel will be required to obtain from Buyer an Electronic Access account per individual, including Buyer Access Controls that may come from Buyer, third parties designated by Buyer or alternate controls subject to Buyer approval. Buyer reserves the right, without notice and in its sole discretion, to terminate and/or block the access of any individual or entity to the Buyer Systems.

Seller acknowledges that the Access Controls are for specific individual use of Seller Personnel only, are not transferable, and shall be maintained in confidence by Seller. Seller shall:

4.1.1. ensure that all Seller Personnel review and agree to abide by the terms of the Contract including this Terms of Use of Boeing Electronic Systems Supplement, prior to being granted Electronic Access;

4.1.2. assign a single focal to initiate requests for Electronic Access for Seller Personnel, coordinate security briefings, maintain records of Seller Personnel granted electronic access, available for validation upon request of Buyer, and coordinate with Buyer regarding actual or potential security breaches;

4.1.3. prevent the loss, disclosure, reverse engineering, sharing with unauthorized Seller Personnel or compromise of Access Controls; and

4.1.4. be responsible for the acts and omissions of all Seller Personnel with respect to their Electronic Access;

4.1.5. immediately notify Buyer if Seller believes that any Access Control has been compromised;

4.1.6. review at least every three (3) months each Seller Personnel's Electronic Access requirements;

4.1.7. promptly submit a written request to Buyer upon the reassignment, resignation, or termination of any Seller Personnel with Electronic Access, to terminate such Electronic Access; and

4.1.8. immediately submit a written notice of name and BEMS ID(s) to Buyer for any Seller Personnel who has Electronic Access to Boeing Systems is terminated for cause by reason of misappropriation of Boeing Proprietary Information or data, or unauthorized access to or use of Boeing systems, or similar reason.

4.2. Seller System Protection: Prior to connecting to Buyer's internal network (either directly at Buyer's site or remotely via SSLVPN or through connect.boeing.com), Seller shall take reasonable steps to protect the confidentiality, integrity and availability of Boeing Systems and information by implementing and maintaining effective controls on all Seller equipment used to connect to Boeing Systems including, without limitation:

4.2.1. Patched and current operating systems and applications – Seller shall subscribe to and apply the vendor's updates;

4.2.2. Anti-malware – Seller devices shall have up-to-date anti-virus protection running with the latest signature files;

4.2.3. Software firewall – Seller shall use an up-to-date version of a software firewall configured to limit ports/protocols to only those necessary (such software firewalls are required even when a local hardware firewall or enterprise firewall is used);

4.2.4. Access Controls – Seller shall use an account/password or token/PIN to access or unlock computing devices; and

4.2.5. Encryption - Whole disk or file/folder encryption shall be used to protect Materials that are being stored locally on the Seller's mobile devices.

4.3. Virtual Office Work: Seller Personnel may access the Boeing systems from locations that have not been assessed (provided they are not public locations and both Buyer and Seller have mutually approved of such locations). Buyer reserves the right to require virtual Personnel to follow virtual office requirements as provided to Seller by Buyer from time to time.

4.4. Export Control. US Trade Control

4.4.1. In order to comply with applicable U.S. export control statutes and regulations, Buyer shall be required to obtain information concerning identity and citizenship, including dual or third country national status, if applicable, or place of birth of Seller Personnel with Electronic Access. Where access is granted, Seller shall be responsible for obtaining all export authorizations required, including where applicable, export authorizations related for Seller Personnel. If related to Electronic Access export authorization(s) are required to allow such Seller Personnel to perform the work to which he or she is assigned, Seller must obtain such authorizations and Seller shall comply with any

additional export control restrictions as required by applicable U.S. export control statutes and regulations.

4.4.2. **TECHNICAL DATA AND SOFTWARE ACCESSED FROM BOEING ELECTRONIC SYSTEMS MAY BE SUBJECT TO UNITED STATES GOVERNMENT EXPORT CONTROL REGULATIONS IN ACCORDANCE WITH THE DEPARTMENT OF STATE, INTERNATIONAL TRAFFIC IN ARMS REGULATIONS ("ITAR"), OR DEPARTMENT OF COMMERCE, EXPORT ADMINISTRATION REGULATION ("EAR"), AND MAY NOT BE EXPORTED, RELEASED OR DISCLOSED TO FOREIGN PERSONS, WHETHER LOCATED INSIDE OR OUTSIDE THE U.S. WITHOUT PRIOR APPROVAL FROM THE U.S. GOVERNMENT. VIOLATIONS OF EXPORT LAWS INVOKE SEVERE FINES AND PENALTIES FOR BOTH INDIVIDUALS AND THE COMPANIES THEY REPRESENT.**

4.5. Export Control. Non-US Trade Control

4.5.1. In order to comply with applicable international trade control statutes and regulations, Buyer shall be required to obtain information concerning identity and citizenship, including dual or third country national status, if applicable, or place of birth of Seller Personnel with Electronic Access. Where access is granted, Seller shall be responsible for obtaining all trade control authorizations required, where applicable, for all Seller Personnel, including to allow such Seller Personnel permission to perform the work to which he or she is assigned, and Seller shall comply with any additional trade control restrictions as required by applicable jurisdiction export control statutes and regulations.

4.5.2. **TECHNICAL DATA AND SOFTWARE ACCESSED FROM BOEING ELECTRONIC SYSTEMS MAY BE SUBJECT TO GOVERNMENT TRADE CONTROLS IN ACCORDANCE WITH IMPORT AND EXPORT REGULATIONS IN AFFECTED JURISDICTIONS AND MAY NOT BE IMPORTED, EXPORTED, RELEASED OR DISCLOSED TO UNAUTHORIZED PERSONS, WITHOUT PRIOR APPROVAL FROM THE AFFECTED GOVERNMENT. VIOLATIONS OF TRADE CONTROL LAWS INVOKE SEVERE FINES AND PENALTIES FOR BOTH INDIVIDUALS AND THE COMPANIES THEY REPRESENT.**

5. Seller Security Controls. Seller shall implement and maintain reasonable controls to prevent any Unauthorized Use, Security Breaches, or loss of Materials. Without limiting the foregoing, Seller shall:

5.1. have implemented for Seller Systems a policy that adopts Information Security Management principles in accordance with ISO/IEC 27001:2013;

5.2. implement and maintain security controls no less comprehensive than either of the latest two versions of the CIS Controls for Effective Cyber Defense as found at https://www.cisecurity.org/critical-controls.cfm;

5.3. comply with Buyer requirements in the use of and strength of encryption, but use encryption no less than that required by law, regulation, or government standard, based on the sensitivity of the Materials involved in the Contract; and follow guidance for sending and receiving encrypted email per http://www.boeingsuppliers.com;

5.4. perform background checks on Seller Personnel in accordance with the terms herein or terms as indicated within the Statement of Work (and any relevant terms included in a Contract) and provide Buyer details on the extent of the background check process and criteria, including any change or variation to such process or criteria due to restrictions imposed by applicable laws;

5.5. provide Seller Personnel with current and relevant security education with respect to their obligations hereunder; and

5.6. use at least the same effort that Seller uses to protect own proprietary and confidential information, and in no event less than a reasonable amount of effort, to enforce Seller's obligations under this Section 5 against current and former employees.

6. External Hosting Requirements.

6.1. Before Seller places any computing application or Materials on any system not owned or managed by Buyer for purposes of Buyer or a third party access ("Hosted Materials"), Seller shall:

6.1.1. either (i) have current certification to ISO 27001; (ii) have current certification to FedRAMP; or (iii) have conducted a SOC 2 Type II audit within the last two years with results reasonable satisfactory to Buyer; and

6.1.2. establish to Buyer's reasonable satisfaction the security of the Hosted Materials, including by:

6.2. providing to Buyer vulnerability assessments conducted by a third party within the past two years which include (i) application vulnerability assessments, including static and dynamic code analysis (e.g., Veracode SAST/DAST); (ii) network and host scans, including security policy implementation, configurations, patching, listening ports, and protocols; and (iii) penetration testing, including "white hat" attempts to gain access by subverting security controls; and

6.3. providing information requested by Buyer about Seller's structured approach to identifying and mitigating computing security risks through modeling the system and data flows (e.g., STRIDE Threat Model).

6.4. While Seller hosts any computing application or Materials on any system not owned or managed by Buyer for purposes of Buyer or a third party access, Seller shall:

6.4.1. either (i) maintain current certification to ISO 27001; (ii) maintain current certification to FedRAMP; or (iii) conduct a SOC 2 Type II audit at least every two years with results reasonably satisfactory to Buyer;

6.4.2. at Buyer's request, establish to Buyer's reasonable satisfaction the security of the Hosted Materials, including by:

6.5. providing to Buyer vulnerability assessments conducted by a third party at least every two years which include (i) application vulnerability assessments, including static and dynamic code analysis (e.g., Veracode SAST/DAST); (ii) network and host scans, including security policy implementation, configurations, patching, listening ports, and protocols; and (iii) penetration testing, including "white hat" attempts to gain access by subverting security controls; and

6.6. providing information requested by Buyer about Seller's structured approach to identifying and mitigating computing security risks through modeling the system and data flows (e.g., STRIDE Threat Model); and

6.6.1. promptly notify Buyer in writing about any material adverse change to the ongoing effectiveness of controls that protect any Hosted Materials.

7. Information Security Assessments.

7.1. Within thirty (30) days of the effective date of the Contract, Seller shall (i) contact Boeing Information Security at suppliercybersecurity@boeing.com for access to the Exostar Cybersecurity Questionnaire ("CSQ") described at www.exostar.com/PIM/Cybersecurity; (ii) complete the CSQ; and (iii) authorize Boeing to review any CSQ completed by Seller.

7.2. Seller grants Buyer, and its authorized representatives, permission to view all books, reports, records, procedures, and information related to or about the Seller Systems, at any time during the term of the Contract and with reasonable advance notice, in order to assess Seller's compliance with this Supplement ("Assessment"), including Seller's implementation and maintenance of security controls no less comprehensive than the either of the latest two versions of the CIS Controls for Effective Cyber Defense as found at www.counciloncybersecurity.org.

7.3. If (i) Buyer determines in connection with any Assessment that a material vulnerability exists in the Seller Facilities or the Seller Systems or that Seller has otherwise failed to perform any of its obligations under this Supplement; and (ii) Buyer notifies Seller in writing of such vulnerability or Seller's breach of this Supplement, then Seller shall promptly develop a corrective action plan. Any such corrective action plan shall be created in cooperation with Buyer and is subject to Buyer's written approval. Seller shall implement the corrective action plan at its sole expense.

8. Prohibited Use. Seller shall not, unless authorized in writing by Buyer:

8.1. export or save any Materials from the Boeing Systems except in support of the work to be performed under this Contract;

8.2. make any derivative uses of the Boeing Systems or the Materials except in support of the work to be performed under this Contract;

8.3. in any manner transfer any computing application or Boeing Materials to an external system;

8.4. use any data mining, robots, or similar data gathering and extraction methods;

8.5. use any frame or framing techniques to enclose any Materials found on the Boeing Systems;

8.6. through reverse engineering, decompiling, or disassembling any portion of the Access Controls, access or attempt to access any unauthorized Materials or restricted portions of the Boeing Systems, or remove any restrictive markings; or

8.7. access the Boeing Systems through any mechanism other than the authorized Access Controls.

9. Security Breach Notification.

9.1. Seller hereby represents, warrants and covenants that it is and shall remain in compliance with all applicable laws that require notification of Security Breach.

9.2. If Seller discovers or is notified of a Security Breach, Seller shall immediately:

9.2.1. cease access to any Materials that are the subject of the Security Breach and shall not review any unauthorized Materials; and

9.2.2. notify Buyer of such Security Breach and notify Buyer of the Materials involved.

9.3. If Buyer's Materials were in the possession of Seller when Seller discovers or is notified of a Security Breach, Seller shall:

9.3.1. investigate and take reasonable steps to cure the Security Breach;

9.3.2. except with respect to a Security Breach caused by Buyer, provide Buyer with assurance satisfactory to Buyer that such Security Breach will not recur;

9.3.3. take any other reasonable steps determined by and provided in writing by Buyer's related to the incident; and

9.3.4. assist Buyer in investigating, remedying, and taking any other action Buyer reasonably deems necessary to address such Security Breach, including related to any dispute, inquiry, or claim related to such Security Breach.

9.4. Seller shall make the notification required in this Section 9 by immediately complying with the notice requirements in the Contract, and sending email message to abuse@Boeing.com (or any other address specified in writing by Buyer) setting forth the information required in this Section 9. The Seller shall copy the Buyer procurement agent on all related email notifications.

9.5. In addition to any other rights and obligations set forth in a relevant Contract, Seller agrees to permit Buyer to review its security control procedures and practices via physical or Electronic Access by Buyer, including access to Seller facilities in which Seller Systems controlled by Seller are located, as well as any and all premises where maintenance, storage or backup activities are performed.

9.6. Any material breach of this Section 9 by Seller may be considered a default for which Buyer may suspend or revoke Electronic Access.

9.7. Seller acknowledges that any attempts by Seller or any Seller Personnel to circumvent any security measures designed to prevent unauthorized access to the Boeing Systems may be subject to criminal or civil penalties under the U.S. Federal Computer Fraud and Abuse Act and other applicable laws and regulations. In addition to any other remedy available to Buyer under the Contract, or available to Buyer under law or equity, Seller and Buyer hereby agree that Buyer shall be entitled to injunctive relief because a breach of any provision related to Electronic Access may result in irreparable harm to Buyer or its affiliates, for which monetary damages may not provide a sufficient remedy, Buyer may seek both monetary damages and equitable relief.

10. DFARS 252.204-7012 Attestation

DFARS 252.204-7012 Attestation applies when Controlled Unclassified Information (CUI) and/or Covered Defense Information (CDI), as defined by DFARS 252.204-7012, is stored, processed, or transmitted using Seller's provided cloud services.

When Seller provides cloud services to Buyer for the storing, processing, or transmitting of CUI and/or CDI, but are not providing an environment for the specific use by the U.S. Government, Seller shall implement security controls that are equivalent to each of the U.S. Government Federal Risk and Authorization Management Program Moderate baseline controls.

Seller should make every effort to review and understand their obligations under DFARS clause. Seller makes this attestation based upon Seller's understanding of DFARS clause 252.204-7012 and the FedRAMP Moderate baseline controls.

10.1. Seller's FedRAMP moderate equivalent cloud computing environment shall comply with subsections (c) through (g) of DFARS 252.204-7012, dated October 2016, as follows:

10.1.1. Seller shall report cyber incidents to Buyer. Buyer [Contractor per DFARS] is responsible for reporting the cyber incident to the DoD. This includes cyber incidents that occur within a Sellers [subcontractor per DFARS] cloud services environment, Subsection (c).(1) Cyber incident reporting requirement).

10.1.2. Subsection (d) Malicious software – no exceptions.

10.1.3. Seller shall preserve and protect images of known affected Seller Information Systems identified in their review for evidence and all relevant forensic information for at least 90 days from the date the cyber incident was reported to Buyer to allow DoD to request media or decline interest, Subsection (e) Media preservation and protection.

10.1.4. Seller shall, upon request, provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis Subsection (f) Access to additional information necessary for forensic analysis.

10.1.5. Seller shall provide, when required by DoD and upon request by Buyer, damage assessment information to Buyer and to DoD, Subsection (g) Cyber incident damage assessment activities.

11. Seller Software/Code Security

11.1. Seller Software/Code Security applies to all forms of Cyber Services where Code is provided for use on Buyer Information Systems. Seller agrees that:

11.2. Seller shall not deliver any Code to Buyer prior to the code assessment completion

11.3. Seller shall ensure software/code assessments are conducted by a third-party assessment organization mutually agreed to by Seller and Buyer;

11.4. Seller shall not deliver Code containing defects that exceed a Common Vulnerability Scoring System (CVSS), score of Medium or higher;

11.5. Seller shall begin remediation of Seller Code defects from time of either self-discovery, public disclosure, or Buyer notification to Seller, whichever occurs first.

11.6. Prior to delivery of Code updates containing material changes (e.g., major version release), Seller shall:

11.7. Provide current CVSS scoring documentation to Buyer;

11.8. Provide software bill of materials showing a list of all third-party party software components, dependencies, and versions. Third-party software includes, but are not limited to, all open source software and all commercial off-the-shelf software components;

11.9. Seller shall maintain throughout the Term of the Agreement a CVSS score no greater than medium;

11.10. Seller shall implement remediation actions (e.g., deliver patch, updated code) to Buyer's satisfaction within the timelines indicated below or as otherwise mutually agreed to by Seller and Buyer and documented in writing;

11.11. Security defects discovered after initial product delivery are remediated for the life of the software contract using the following table or by an alternative timeframe approved in writing by Boeing.

11.12. 72 hours to deliver patch for any CVSS score of Critical

11.13. 72 hours to deliver patch for any Remote Code Execution (RCE) vulnerability

11.14. 30 days to deliver patch for vulnerability of CVSS score of High

12. Indemnification, Disclaimer, and Exclusion of Liability.

12.1. Seller shall indemnify, defend, and hold harmless Boeing its respective officers, directors, shareholders employees, subcontractors, agents, suppliers and assignees (collectively, the "Indemnified Parties") from and against any and all third-party liabilities, obligations, losses, claims, damages, costs, charges, and other expenses of any kind (including, without limitation, reasonable attorneys' fees and legal expenses) that arise out of or relate to (a) any failure by Seller or any of its subcontractors, or any Seller Personnel, to comply with any obligation under these Terms or (b) the breach of any representation and warranty herein. Boeing may participate in the defense and settlement of any claim for which it is entitled to indemnification hereunder, using attorneys selected by Boeing, at Seller's expense.

12.2. **SELLER HEREBY WAIVES, RELEASES AND RENOUNCES ALL WARRANTIES, OBLIGATIONS AND LIABILITIES OF BOEING AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES AGAINST BOEING, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS, MATERIALS AND ANY INFORMATION, GOODS, SERVICES, OR OTHER THINGS PROVIDED PURSUANT TO THIS AGREEMENT. BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS, AND MATERIAL ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS AND BOEING MAKES NO REPRESENTATION OR WARRANTY AS TO THE COMPLETENESS OR ACCURACY THEREOF. TO THE FULLEST EXTENT PERMITTED BY LAW, SELLER (AND SELLER'S SUBSIDIARIES AND AFFILIATES, IF ANY) HEREBY WAIVE, RELEASE AND RENOUNCE ALL WARRANTIES, OBLIGATIONS AND LIABILITIES OF BOEING AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES AGAINST BOEING, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS AND MATERIALS, EVEN IF BOEING HAS BEEN ADVISED OF THE POSSIBILTY OF ANY DAMAGES, INCLUDING WITHOUT LIMITATION: (A) ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, (B) ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE, (C) ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN CONTRACT OR TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING, AND (D) ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OF OR DAMAGE TO ANY PROPERTY BELONGING TO SELLER OR SELLER PERSONNEL.**

12.3. **BOEING SHALL HAVE NO OBLIGATION OR LIABILITY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING), OR OTHERWISE, FOR LOSS OF USE, REVENUE OR PROFIT OR FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES WITH RESPECT TO BOEING SYSTEMS, ELECTRONIC ACCESS, ACCESS CONTROLS, MATERIALS AND ANY INFORMATION, GOODS, SERVICES, OR OTHER THINGS PROVIDED PURSUANT TO THIS AGREEMENT. THIS PROVISION SHALL SURVIVE TERMINATION OR CANCELLATION OF THIS AGREEMENT.**

12.4. For the purpose of this Section 12, "Boeing" includes The Boeing Company, its divisions, subsidiaries, the assignees of each, subcontractors, suppliers and affiliates, and their respective directors, officers, employees and agents.