Information Technology Terms

These terms apply to you and to your contract(s) with Tennessee Valley Authority ("TVA") to the extent that your work involves providing, servicing, or accessing one or more of the following: IT Work, Operational Technology, TVA Information Systems, or TVA Networks, as defined herein.

Definitions

a. "ByteDance Limited Products" means the social networking service TikTok or any successor application or service of TikTok developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

b. "Contract Information" means any non-public information related to the contracts with TVA and any work performed thereunder, including but not limited to any TVA Confidential Information disclosed to you.

c. "Cyber Asset" means any programmable electronic device, including hardware, software, information, or any of the foregoing, which are components of such devices or enable such devices to function.

d. "Harmful Code" means any computer instructions, circuitry or other technological means whose purpose is to disrupt, damage or interfere with information systems or other systems and data, including, without limitation, any automatic restraint, time-bomb, trap-door, virus, worm, Trojan horse, time lock, clock or any other harmful, malicious or hidden procedure, routine or mechanism.

e. "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Contract Information.

f. "IT Work" means the total of all hardware, software, software licenses, networks, cloud services, telecom, servers, databases, electronic programs, and related actions, management, services, Operational Technology (as defined herein), records (electronic or physical) or responsibilities, that you will develop, update, upgrade, grant, deliver, transmit, perform, or provide to TVA.

g. "Kaspersky Product" means any software code, or any information security product, solution, network, system, or service, that is or has been supplied (directly or indirectly) by AO Kaspersky Lab or any of its predecessor entities or its affiliates (including, without limitation, Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc.), or any entity in which one or more of the foregoing has majority ownership or voting control.

h. "Network" means a system implemented with a collection of connected components, including routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

i. "NIST" means the National Institute of Standards and Technology, a federal agency within the U.S. Department of Commerce.

j. "Operational Technology" means programmable systems or devices that interact with the physical environment, or manage devices that interact with the physical environment.

k. "Personally Identifiable Information" or "PII" means any information or representation of information, in any media, which: (i) potentially can be used, directly or indirectly, to uniquely identify, contact (physically or online), or locate a single individual (e.g., age, gender, or weight), (ii) if disclosed without prior written authorization, could create a substantial risk of identity theft from such individual (e.g., social security number, bank account number, or home address), or (iii)

a Governmental Authority intends to use to indirectly identify specific individuals in conjunction with other data elements, such as a combination of gender, race, birth date, geographic indicator, and other descriptors.

l. "Vulnerability(ies)" means any publicly disclosed material defect or compromise to the cybersecurity of your or your subcontractor(s)' product or service provided, serviced, or delivered to TVA as part of the IT Work.

Warranties and Product Integrity

a. You represent and warrant that IT Work and any media used to distribute IT Work:

   1. do not contain Harmful Code at the time of initial delivery or at the time of updates or upgrades. You shall cooperate with TVA, and shall make commercially reasonable efforts, including use of an industry standard scanning tool, to prevent the introduction and proliferation of Harmful Code into TVA's Information Systems, including software and hardware necessary to operate such Information Systems and the TVA Network(s) on which such Information Systems reside;

   2. do not contain and have never been affected by input from, included on any required information technology as, and are free from, any Kaspersky Products, ByteDance Limited Products, or any other software products (or combination thereof) that are prohibited by applicable laws, including, without limitation, Department of Homeland Security Directives and Office of Management and Budget memoranda;

   3. will not require the storage, processing, or communication of TVA Contract Information outside of the United States without TVA's prior, written approval; and

   4. will only allow United States Persons, as defined by 22 CFR Part 120.15, or other individuals legally authorized under applicable laws, specifically including Export Control Laws, to access Contract Information and to provide technical support of the IT Work.

b. You shall indemnify and hold TVA harmless from all liabilities resulting from your and your subcontractor(s) failure to comply with subsections a.1, a.2, and a.4 above.

c. You must provide or deliver to TVA work products and services, as applicable, that comply with the requirements stated in subsection (a), above, and the following (as appropriate and specified on work release(s)): (1) for work products delivered physically, in sealed boxes, packaged to indicate that the seal has not been broken, disturbed, or modified, (2) for work products or services delivered electronically, but separately from the work products or services themselves, a list of all delivered files and (i) the sha-1, sha-2 hash values. TVA receiving personnel will verify that either: (x) tamper evident seals of the packaging are intact, or (y) you have provided (by email or otherwise in writing) the information required by subsection (2), above, or (as appropriate) a cryptographic key and access information for the electronic work products or services.

d. The IT Work provided to TVA shall not contain so-called "shrink wrap" or "click wrap" license terms, provided that, if you package or electronically deliver to TVA licenses or versions of IT Work that contain any such "shrink wrap" or "click wrap" license terms, the terms and conditions signed by the parties which specifically include these terms, and the applicable work release apply, and supersede the terms of the "shrink wrap" or "click wrap" license.

e. Within thirty (30) days of entering into a contract with TVA, you shall provide to TVA information or documentation sufficient to enable TVA to determine that appropriate security controls are in place and operating as expected. You shall provide independent testing of those controls, and document and maintain a plan that describes specific measures that it will take to correct any deficiencies found during independent testing. Specifically, you must obtain and provide to TVA, within one year of entering into an contract with TVA, provided that the contract has a term of at

least one year, a complete third party cybersecurity attestation, including but not limited to a Systems and Organization Controls ("SOC") 2 Type 2 Report and an annual SOC 2 Type 2 audit review (a "SOC 2 Report"), or an International Organization for Standardization ("ISO") 27001 Certification and Report and annual ISO 27001 audit review (an "ISO 27001 Report"). If you cannot provide a complete third party cybersecurity attestation, then you must deliver to TVA a self-attestation (compliant with NIST requirements, and reasonably acceptable to TVA in form and substance) documenting your security controls and policies.

f. If required by applicable law (specifically including, for purposes of this Section, Executive Order 14028) or upon TVA's request, you shall (i) provide to TVA or its designated agent a formal record containing the details and supply chain relationship of various components used in building the software provided, commonly known as a Software Bill of Materials ("SBOM"), or (ii) implement or incorporate phishing-resistant multifactor authentication ("MFA") components to the IT Work, or both, as further set forth in an applicable work release.

g. You shall ensure that your subcontractor(s) comply with this Section, and are liable for such subcontractor(s)' failure to comply with this subsection.

Accessible Technology, Software, Web Sites and Services

a. Upon TVA's request, you shall provide TVA with responses to the relevant portions of the Voluntary Product Accessibility Template (VPAT), located at http://www.itic.org/public-policy/accessibility, which will assist TVA in determining your compliance with Section 508 of the Rehabilitation Act, 29 U.S.C. 794d, and the Access Board Standards (see https://www.section508.gov/manage/laws-and-policies/).

b. Unless otherwise approved by TVA's designated representative, all applicable IT Work must comply with Section 508 of the Rehabilitation Act when accessible technology is available in the market and meets TVA's requirements and specifications.

TVA Furnished Information Technology Equipment

a. TVA may elect to furnish TVA-owned information technology equipment ("TVA IT Equipment," as defined herein) for your use if TVA determines that such use is the most cost-effective way to support the your performance of work. For purposes of this Section, TVA IT Equipment means: (a) any equipment or interconnected system or subsystems of equipment that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception of data or information; and (b) computers; ancillary equipment, data communication lines and other communication hardware, software, firmware; or similar equipment identified on work release(s).

b. TVA will deliver any such TVA IT Equipment at the time and location specified in work releases(s), or as otherwise authorized in writing by TVA's designated representative.

c. All TVA IT Equipment, and any services, maintenance or support provided by TVA or third-party contractors relating to such TVA IT Equipment, are provided "AS IS" or on a courtesy basis (as applicable), disclaiming any warranties by TVA or on TVA's behalf.

d. TVA owns and will retain title to all TVA IT Equipment provided to you, including any such equipment that you purchase as agent for TVA, or otherwise on TVA's behalf (if and as authorized by specific work release(s). You shall not use TVA IT Equipment except in direct support of your work for TVA. You assume the risk and responsibility for loss or damage (other than as incident to reasonable usage for purposes of the work) to any TVA IT Equipment after its initial delivery to you, and until its return to TVA.

e. You shall maintain written property control records for all TVA IT Equipment in accordance with sound business practices and will make such records available for TVA inspection, upon TVA's request.

f. Upon completion or termination of work for any reason, you shall follow the instructions of TVA's designated representative regarding the return and disposition of all TVA IT Equipment, and shall return all related records to TVA.

Use of a TVA Information System

a. Your use of a TVA Information System, authorized or unauthorized, constitutes your consent to TVA's monitoring of your or any of yoursubcontractor(s)' use of the relevant TVA Information System. TVA may provide access to its Information System(s) and all related equipment, networks, and network devices (including internet access) only to authorized users for authorized purposes. You are responsible for ensuring that your employees, subcontractor(s), and their agents comply with any applicable TVA procedures, including TVA-SPP-12.001 Acceptable Use of Information Resources.

b. Any of youremployee(s) or subcontractor(s) who seek access to a TVA Information System, or receives a TVA network ID ("Contractor Users"):

1. first shall complete TVA Form 40156 "TVA Contractor and TVA Nuclear Badged Employee Check-In Form Hire and/or Unescorted Nuclear Access Request." Any employee who receives a TVA network ID, or access to a TVA Information System, must complete TVA Form 40157, "TVA Contractor Check-Out Form" upon the completion or termination of his or her work , for any reason; and

2. is subject to and must comply with: (i) the requirements of the United States Citizenship and Immigration Services (USCIS) related to a Contractor User's eligibility to work in the United States, (ii) Export Control Laws (as defined below), and (iii) TVA Police & Emergency Management security screening requirements, as applicable to each Site. You must acquire, verify and maintain appropriate documentation (such as valid U.S. Social Security number(s) and USCIS Form I-9) on all Contractor Users who seek access to a TVA Information System.

c. In order to have and maintain access to TVA Information Systems, all Contractor Users will receive an assigned TVA network ID and must (at minimum) successfully complete required cybersecurity training and testing within 14 days of their receipt of such network ID. After completion of the initial training, Contractor Users must complete required training on an annual basis (before their training anniversary date).

d. Any Contractor User's use of a TVA Information System constitutes your agreement to comply with such system's terms of use. TVA may deny or revoke a Contractor User's access to any TVA Information System if: (1) such Contractor User fails to successfully and timely complete any Security Awareness training, (2) TVA's information or TVA Information Systems are misused or abused, or (3) TVA's terms of service are violated. TVA will not pay or reimburse you, and you shall not claim against TVA for any delays, costs, or other expenses incurred by you or your subcontractor(s), relating to TVA's revocation or denial of system access to a Contractor User.

e. You shall immediately notify TVA in writing whenever you disables electronic access by or for any of your employees or subcontractor(s) to your Information System(s), due to any action that temporarily or permanently severs the employment or subcontracting relationship (including, without limitation, termination, resignation, or suspension) within 24 hours of the action. Upon receipt of such notice from you, TVA will immediately disable the relevant employee(s)' electronic access to TVA Information Systems.

Personally Identifiable Information and Privacy Act

If you or your subcontractor(s) obtain or have access to PII in connection with work performed or delivered to TVA, or if work product or services delivered to TVA contains modules or features that collect or the functionality of which could be updated to collect PII, you shall comply with the TVA terms for Personally Identifiable Information and Privacy Act located at https://www.tva.com/Information/Supplier-Connections/Documents--Referenced-Clauses, as amended from time to time.

External Information Systems

For any Information Systems hosted externally to TVA, by you, your subcontractor(s), or by Cloud Service Provider(s), as part of or incident to your work or services, you shall comply with the TVA terms for External Information Systems located at https://www.tva.com/Information/Supplier-Connections/Documents--Referenced-Clauses, as amended from time to time.

Knowledge Transfer

Upon request or as otherwise set forth in an applicable work release, you shall furnish phase-in training to TVA or third-party contractor personnel upon the expiration or termination of your agreement with TVA, and cooperate with TVA to ensure an orderly and efficient transition of such work.

Vulnerabilities

a. Prior to the performance of any IT Work for TVA, you shall provide summary documentation of any Vulnerability, the potential impact of such Vulnerabilities, and the status of your efforts to mitigate those publicly disclosed Vulnerabilities. You, at your own expense, shall implement any corrective actions, compensating security controls, mitigations, or procedural workarounds, or any of the foregoing, which it recommends as necessary to address the identified Vulnerabilities.

b. Consistent with applicable laws (specifically including NIST's definitions of "critical vulnerabilities" and "high vulnerabilities"), during the performance of any IT Work for TVA, you shall provide remediation or mitigate all identified Common Vulnerabilities and Exposures (CVE) from the date vulnerabilities are formally identified, where applicable: (i) Critical vulnerabilities within 7 calendar days, and (ii) High vulnerabilities within 15 calendar days, unless otherwise directed in writing by TVA's designated representative. Furthermore, you shall make commercially reasonable efforts to prioritize, minimize, and/or remediate any other Known Exploited Vulnerabilities as identified in the Known Exploited Vulnerabilities Catalog maintained by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

Cyber Security Incidents: Notices and Responses

a. In addition to any notice required by your contract(s) with TVA, you agree to notify TVA promptly at (423) 751-4357 and then immediately thereafter by providing a written communication to TVA at CYBERSECURITY@TVA.GOV, whenever you know or reasonably believe that an act or omission by any source has compromised or may adversely affect or breach: (i) the cybersecurity of any IT Work, or (ii) the physical, technical, administrative, or organizational safeguards protecting your Information Systems (any of the foregoing, a "Compromise").

b. Within seven days of notifying TVA of the Compromise, you shall recommend actions that TVA should take on TVA Cyber Assets to reduce the risk of a recurrence of the same or a similar Compromise, including, as appropriate, the provision of action plans and mitigating controls. Unless TVA or its agents negligently caused the Compromise, you are responsible for developing and implementing those action plans and mitigating controls, at your own expense. Regardless of the cause(s) of the Compromise, you shall coordinate with TVA in implementing the action plans and mitigating controls. In addition, you will provide TVA guidance and recommendations for long-

term remediation of any cyber security risks posed to TVA Cyber Assets, and any information necessary to assist TVA in any of its recovery efforts in response to a Compromise.

Remote Access

If the IT Work involves establishment or maintenance of remote access to a TVA Cyber Asset (either interactive or to and from an external Cyber Asset), you shall (i) comply with TVA Cyber Asset requirements and preconditions, and (ii) coordinate with TVA to establish controls that govern any such remote access to TVA Cyber Assets.

Product Lifecycle Notices and Documentation

a. In addition to the warranties stated in the ***Warranties and Product Integrity*** Section, above, you represent and warrants that the planned end-of-life date on your product roadmap for all IT Work provided to TVA is later than the termination date of your contract(s) with TVA, including any optional extensions. Upon TVA's request, you shall supply TVA with all applicable vendor manuals, white papers, support documents, and other documents related to your product lifecycle.

b. You shall notify TVA at least one year in advance of any changes to IT Work that would: (1) diminish, or require TVA to upgrade its Information Systems to maintain, the functionality of the IT Work, or (2) require TVA to transition to a different platform. If you comply with the foregoing notice requirement, TVA may require that you continue to support the then current configuration of the IT Work, and the parties will negotiate an appropriate amount of compensation for such support. If you fail to provide the notice required by this subsection or inform TVA that you cannot or will not continue support of the existing configuration of IT Work, TVA may, in addition to any other remedies, immediately terminate its contract(s) with you and receive a pro-rata refund of all prepaid fees.

Reseller Responsibilities

If you are a reseller of IT Work, then at a minimum, you shall ensure that the separate agreement between you and the original equipment manufacturer or service provider ("OEM") of the IT Work: (1) imposes obligations on you and OEM at least as stringent as those stated in your contract(s) with TVA, and (2) does not impose obligations on TVA that are not stated in your contract(s) with TVA. If and as applicable, you also must notify the OEM that your contract(s) with TVA supersede any conflicting terms in the separate agreement between you and the OEM.