

Information Technology Terms

This Section applies to the extent that Contractor's scope of 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 this Contract and the Work, including but not limited to any TVA Confidential Information disclosed to Contractor.
- 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. "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 Contractor will develop, update, upgrade, grant, deliver, transmit, perform, or provide to TVA under this Contract.
- f. "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.
- g. "Network" means a system implemented with a collection of connected components, including routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
- h. "NIST" means the National Institute of Standards and Technology, a federal agency within the U.S. Department of Commerce.
- i. "Operational Technology" means programmable systems or devices that interact with the physical environment, or manage devices that interact with the physical environment.
- j. "Vulnerability(ies)" means any publicly disclosed material defect or compromise to the cybersecurity of Contractor's or its Subcontractor(s)' product or service provided, serviced, or delivered to TVA as part of the IT Work.

Warranties and Product Integrity

- a. Contractor represents and warrants 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;
 2. do not contain and have never been affected by any Kaspersky Products, ByteDance Limited Products, or any other software products (or combination thereof) that are prohibited by Applicable Laws;
 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 not allow Foreign Persons, or other individuals not authorized under Applicable Laws, to access Contract Information or provide technical support of IT Work.
- b. Contractor shall indemnify TVA from all liabilities resulting from Contractor's and its subcontractor(s) failure to comply with subsections a.1, a.2, and a.4 above.
 - c. Contractor must provide or deliver to TVA Work Products that comply with the requirements stated in subsection (a), above, and any additional security and access controls and protocols specified on Work Release(s). Prior to implementation or installation (as appropriate) of Work Products, Contractor shall provide to TVA information or documentation sufficient to enable TVA to determine that appropriate security controls are in place and operating as expected.
 - d. The IT Work shall not contain so-called "shrink wrap" or "click wrap" license terms, or other terms of service that conflict with this Contract. This Contract and the applicable Work Release supersede any such conflicting terms.
 - e. As required by Applicable Laws (specifically including, for purposes of this Section, Executive Order 14028), Contractor shall (i) provide a self-attestation, or its equivalent, from the software producer in accordance with the Cybersecurity Infrastructure and Security Agency (CISA)-issued "Common Form," reference <<https://www.tva.com/information/supplier-connections/for-technology-providers>>, and (ii) implement or incorporate phishing-resistant multifactor authentication ("MFA") components to the IT Work. Additionally, upon request from TVA or its designated agent, Contractor shall provide a formal record containing the details and supply chain relationship of various components used in building the software provided under this Contract, commonly known as a Software Bill of Materials ("SBOM").
 - f. Contractor shall ensure that its Subcontractor(s) comply with this Section, and is liable for such Subcontractor(s)' failure to comply with this subsection.

Accessible Technology, Software, Web Sites and Services

- a. Upon TVA's request, Contractor 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 Contractor's 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 the Contracting Officer, 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 Work requirements and specifications.

TVA Furnished Information Technology Equipment

- a. "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. If TVA decides to deliver to Contractor any TVA IT Equipment for Contractor's use in connection with the Work, TVA retains title at all times to such TVA IT Equipment. Any services, maintenance or support related to TVA IT Equipment, or which third-party contractors may provide to Contractor, are provided "AS IS", disclaiming any warranties by TVA or on TVA's behalf. Contractor: (1) shall not use TVA IT Equipment except in direct support of its Work; (2) assumes 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 Contractor, and until its return to TVA, and (3) 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.
- c. Upon completion of Work or termination of this Contract for any reason, Contractor shall follow the instructions of the Contracting Officer regarding the return and disposition of all TVA IT Equipment, and shall return all related Records to TVA's CTS.

Contractor Use of TVA Information System

- a. Contractor's use of a TVA Information System, authorized or unauthorized, constitutes Contractor's consent to TVA's monitoring of Contractor's or any Subcontractor(s)' use of the relevant TVA Information System. TVA may provide access to its Information System and all related equipment, networks, and network devices (including internet access) only to authorized users for authorized purposes. Contractor is responsible for ensuring that its employees, its Subcontractor(s), and their agents comply with any applicable TVA procedures, including TVA-SPP-12.001 Acceptable Use of Information Resources.
- b. Any Contractor employee or Subcontractor(s) that seek(s) 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 of his or her Work, or the termination of this Contract or the relevant subcontract(s), 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. Contractor 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's Information System constitutes Contractor's 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 Contractor, and Contractor shall not claim against TVA (under the Changes Section of this Contract, or otherwise), for any delays, costs, or other expenses incurred by Contractor or Subcontractor(s), relating to TVA's revocation or denial of system access to a Contractor User.

- e. Contractor shall immediately notify the CTS or designee in writing whenever it disables electronic access by or for any of its employees or Subcontractor(s) to a Contractor's Information System, due to any action that temporarily or permanently severs the employment or Subcontractor relationship within 24 hours of the action. Upon receipt of such notice from Contractor, TVA will immediately disable the relevant employee(s)' electronic access to TVA Information Systems.

Personally Identifiable Information and Privacy Act

If Contractor or its Subcontractor(s) obtain or have access to PII in connection with Work performed or delivered under this Contract, or if Work Product delivered to TVA contains modules or features that collect or the functionality of which could be updated to collect PII, Contractor 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 Contractor, its Subcontractor(s), or by Cloud Service Provider(s), as part of or incident to Contractor's Work, Contractor 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, Contractor shall furnish phase-in training to TVA or third-party contractor personnel upon the expiration or termination of this Contract for any reason, and cooperate with TVA to ensure an orderly and efficient transition of such Work.

Vulnerabilities

Consistent with Applicable Laws (specifically including NIST's definitions of "critical vulnerabilities" and "high vulnerabilities"), during the performance of any IT Work under this Contract, Contractor shall provide summary documentation of any Vulnerability, the potential impact of such Vulnerabilities, and the status of Contractor's efforts to mitigate those publicly disclosed Vulnerabilities. Contractor, at its 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.

Cyber Security Incidents: Notices and Responses

- a. In addition to any notice required under this Contract, Contractor shall notify TVA promptly at (423) 751-4357 and then immediately thereafter by providing a written communication to TVA at CYBERSECURITY@TVA.GOV, whenever Contractor knows or reasonably believes 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 Contractor's Information Systems (any of the foregoing, a "Compromise").
- b. Within seven days of notifying TVA of the Compromise, Contractor 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, Contractor is responsible for developing and implementing those action plans and mitigating controls, at its expense. Regardless of the cause(s) of the Compromise, Contractor shall coordinate with TVA in implementing the action plans and mitigating controls. In addition, Contractor 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), Contractor shall (i) comply with TVA Cyber Asset requirements and preconditions, and (ii) coordinate with TVA's CTS 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, Contractor represents and warrants that the planned end-of-life date on Contractor's product roadmap for all IT Work provided under this Contract is later than the termination date of this Contract, including any optional extensions. Upon TVA's request, Contractor shall supply TVA with all applicable vendor manuals, white papers, support documents, and other documents related to its Product Lifecycle.
- b. Contractor 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 Contractor complies with the foregoing notice requirement, TVA may require that Contractor continue to support the then current configuration of the IT Work until this Contract's termination date, and the parties will negotiate an appropriate Change Notice, consistent with this Contract's **Changes** Section. If Contractor fails to provide the notice required by this subsection or informs TVA that it cannot or will not continue support of the existing configuration of IT Work, TVA may, in addition to any other remedies, terminate this Contract for default.

Reseller Responsibilities

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

Artificial Intelligence

If Contractor offers Artificial Intelligence (AI) tools or services, or provides Work under this Contract that includes AI features, or was otherwise developed, wholly or with the assistance of AI technology, then the TVA Artificial Intelligence Terms, located at <https://www.tva.com/information/supplier-connections/documents-referenced-clauses>, as amended from time to time, will apply. If any conflict exists between TVA's Artificial Intelligence Terms and any Contractor AI terms of use, the former will supersede and govern the latter.