12.1 External Information Systems (1211)

a. This Section applies to any Information Systems external to TVA, which are hosted by Contractor, its Subcontractor(s), or by Cloud Service Provider(s) (as those terms are defined herein), as part of or incident to Contractor's Work ("External Information Systems").

b. Basic Safeguarding of Covered Contractor Information Systems. Contractor and its Subcontractor(s) must comply with specific safeguarding requirements stated in Applicable Laws and by Governmental Authorities, which apply to External Information Systems. In addition to the foregoing, Contractor shall apply the following minimum security controls to all External Information Systems:

1. Establish and identify users, processes acting on behalf of users, or devices (including other Information Systems), who and which are authorized by TVA, or authorized by Contractor and approved by TVA, to access the External Information System(s) ("Authorized Users").

2. Limit External Information System access to Authorized Users, and to the types of transactions and functions that Authorized Users are permitted to execute.

3. Authenticate (or verify) the identities of all Authorized Users as a prerequisite to allowing access to Information Systems, and limit Authorized Users' connections to and use of external information systems through the External Information Systems.

4. Limit physical access to External Information Systems, related equipment, and the respective operating environments, to Authorized Users, and escort visitors and monitor visitor activity, maintain audit logs of physical access, and control and manage devices that can be used to gain physical access to External Information Systems.

5. Sanitize or destroy External Information System media containing Contract Information before disposal or release for reuse.

6. If the External Information System is publicly accessible, in whole or in part, control information posted on or processed by its publicly accessible portion(s).

7. Implement subnetworks for publicly accessible system components that are physically or logically separated from the External Information System(s)' internal networks.

8. Perform periodic scans of the External Information System and real-time scans of files from external sources as files are downloaded to, opened in, or executed by or through the External Information System(s).

9. Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the External Information Systems.

10. Ensure the integrity and authenticity of the External Information System(s), and all associated security patches, through physical or logical mechanisms, or both mechanisms, as appropriate to the nature of the External Information System(s).

c. Cloud Services. If and to the extent that Contractor's Work includes the provision of Cloud Computing services to TVA, by it, its Subcontractor(s), or its or their agent(s) (individually and collectively referred to in this Section as a Cloud Service Provider, or "CSP"), the CSP will comply with the following in connection with its performance of Cloud Computing services ("Cloud Services") as part of this Contract's Work:

1. Upon prior written notice to Contractor, and at a mutually agreeable time, TVA may perform a virtual or onsite information security assessment of relevant External Information Systems associated with the Cloud Services.

2. The CSP will use Contract Information only for the purpose of meeting its obligations set forth in this Contract and any applicable Work Release. The CSP will also make Contract Information held or stored by the CSP, or its agent(s) available for retrieval for no less than 90 days after the termination of this Contract (for any reason), and promptly after the later of termination or TVA's retrieval of its information, the CSP, unless otherwise agreed upon by the parties in writing or required by Applicable Law, will destroy any Contract Information in its possession or control. The CSP must certify in writing that the Contract Information has been so destroyed, unless TVA elects to waive (in writing) such certification requirement.

3. The CSP will notify TVA accordingly in the following Cloud Services situations: (a) at its earliest possible opportunity of any suspected security incident or the attempted access of Contract Information, and (b) no later than one hour of any confirmed security incident or the unauthorized access or attempted access of Contract Information. The one-hour time frame begins once a security incident has been confirmed, and does not include the time it takes to confirm that a security incident has occurred. The CSP must effect such notice by telephone to the Contracting Officer, and to the TVA ITCO at (423) 751-4357, and then immediately thereafter by providing a written communication to TVA at CYBERSECURITY@TVA.GOV, summarizing the incident and providing a designated CSP contact for the incident.

4. Document Information System connections, as requested by TVA, with an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or both. The CSP shall transmit data externally only through connections that use secure communications (e.g., TLS, HTTPS/SSL, SSH, IPSec). Only ciphers that are generally recognized as safe may be used. Deprecated ciphers are prohibited.

5. Upon TVA's written request, the CSP shall provide relevant security logs that can be integrated into TVA's security suite utilizing RFC-compliant, TLS-protected syslog or service vendor-provided API connectors.

6. The CSP will use reasonable efforts to limit the interruption of External Information Systems and operation and maintenance times. The CSP will notify TVA in writing, at least 48 hours in advance, of any planned maintenance that could interrupt External Information Systems.

d. Any Contractor providing Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS), each a "Cloud Information System", shall provide evidence of authorization by the Federal Risk and Authorization Management Program (FedRAMP) prior to TVA's use. Any Cloud Information System not authorized by FedRAMP must provide: (i) a self-attestation affirming compliance with the NIST standards referenced in the Warranties and Product Integrity subsection of this Information Technology Section, and (ii) proof reasonably satisfactory to TVA that Contractor has implemented an appropriate control baseline based on latest version of the Federal Information Processing Standard (FIPS) 200.

e. Contractor shall not connect any TVA IT Equipment to an External Information System without the prior, written approval of TVA's CTS. If TVA's CTS provides such approval, Contractor must, at its sole cost, ensure that any TVA IT Equipment that is connected with or integrated into a External Information System complies with the applicable requirements 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).

f. Any reference in this Section to a NIST Special Publication (SP), Applicable Laws, or TVA or other federal standards, programs, memoranda or guidance, is to the latest issued or most recently amended version of such documents or requirements.

g. Subcontracts. Contractor shall include the substance of this Section, including this subsection (h), in subcontracts under this Contract, in which Subcontractor(s) may process, store or transmit Contract Information through an External Information System.