

Personally Identifiable Information and Privacy Act

- a. Contractor shall obtain, access, use, receive, back-up, protect as Confidential Information, maintain, transmit, store, and disclose personally identifiable information ("PII") at all times in compliance with applicable laws and regulations, including without limitation the federal Privacy Act of 1974, 5 U.S.C. § 552a ("Privacy Act"). If Contractor requests PII from any individual, Contractor shall provide a Privacy Act statement with such request or directly to such individual, which includes a notice of the expected routine uses of such information. PII may also meet the definition of Protected Health Information ("PHI") and be subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the privacy and security rules promulgated thereunder. In the event Contractor receives PHI from TVA or creates PHI on behalf of TVA, Contractor shall comply with the applicable HIPAA Business Associate Agreement.
- b. If an event has or could have resulted in the unauthorized access to, loss, theft, or damage to PII (hereinafter, "security incident"), Contractor shall:
 1. immediately notify TVA in writing, and: (i) (at minimum) identify in such notice to the extent known, the information involved in the security incident, the timing and place of the security incident, the cause of the incident, and the steps being taken to mitigate any harm or damage caused by the security incident; and (ii) after such notice, as required by TVA, provide timely and regular updates regarding the security incident, and cooperate with TVA-designated personnel to mitigate any risks to information systems, or of further unauthorized disclosure of PII, posed by the security incident; and
 2. cooperate with TVA in any investigation or legal proceedings relating to a security incident.
- c. In the event of any security incident, TVA may, at its option, perform an independent risk analysis of the security incident to determine the level of risk and potential harm associated with the security incident. Contractor agrees to fully cooperate with and assist in this risk analysis.
- d. Within 90 days of the expiration or termination of a contract with TVA or upon the conclusion of Contractor's data retention policy which shall not exceed one year from the contract's expiration or termination, Contractor shall destroy or return to TVA all PII received or obtained while performing work under the applicable contract.
- e. In the event of a loss or compromise of PII held by Contractor, its agents, or its Subcontractor(s), under this Contract, Contractor must (by written notice to such person(s) whose PII was lost or compromised, subject to TVA's review and approval), at its sole cost, and without cost or liability to TVA, offer to provide the following services: (1) 12 months of credit monitoring, and (2) for serious or large incidents as defined by TVA, call center help desk services.