

Pub. 1075 Exhibit 7 Safeguarding Contract Language Obligations

To the extent that this Pub. 1075 Exhibit 7 Safeguarding Contract Language Obligations (the "Attachment") is incorporated into the Contract by reference, the Vendor agrees to comply with the obligations set forth in this Attachment. This Contract Attachment supplements and is made a part of the Contract between the purchasing Agency and the Vendor.

To the extent that Vendor provides notice that it does not accept an amended Attachment, any agreed alteration not part of the then current Attachment shall have no force or effect until the agreed alteration is reduced to a Contract amendment and signed by the Vendor and the purchasing Agency. In such a case, the existing Attachment will continue to remain a part of the Contract until such time as the parties agree to a newly amended Pub 1075 Exhibit 7 compliance attachment.

I. PERFORMANCE

In performance of this Contract, the Vendor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

- (1) All work will be performed under the supervision of the Vendor.
- (2) The Vendor and Vendor's officers or employees to be authorized access to federal and/or state tax information ("FTI") must meet background check requirements defined in IRS Publication 1075. The Vendor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection or disclosure of FTI to anyone other than the Vendor or the Vendor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The Vendor will certify that FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Vendor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Vendor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the Vendor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this Contract will be subcontracted without the prior written approval of the IRS.

(9) Vendor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Vendor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this Contract assumes toward the Vendor, and the subcontractor shall assume toward the Vendor all the same obligations, duties and responsibilities which the Vendor assumes toward the agency under this Contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Vendor hereunder by the same terms and conditions by which the Vendor is bound and obligated to the agency under this Contract.

(12) For purposes of this Contract, the term "Vendor" includes any officer or employee of the Vendor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the Contract if the Vendor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a Vendor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a Vendor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a Vendor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(4) Additionally, it is incumbent upon the Vendor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Vendor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(5) Granting Vendor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. Vendor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, Vendor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Pub. 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the Vendor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Vendor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Vendor is found to be noncompliant with FTI safeguard requirements.