# VR Standards for Providers (VR-SFP) Chapter 3: Basic Standards

The following sections in the VR-SFP have been revised; these requirements are effective September 4, 2018.

## 3.2 Insurance Requirements

All contractors subject to the Standards for Providers (VR-SFP) must provide proof of insurance, as required, to the assigned Texas Workforce Commission (TWC) contract manager and regional program specialist.

TWC VR requires the following kinds of insurance:

* Garage liability insurance for vehicle modification providers, as required per contract;
* Auto liability insurance for providers who choose to transport customers in motorized vehicles. Transportation of VR customers is not required, but if done, contractors must meet the minimum liability requirements of the Texas Department of Insurance, and keep records of staff who transport customers in vehicles.

When insurance is required, the contractor submits the form [DARS3445, Provider Insurance Verification](https://twc.texas.gov/forms/index.html), with evidence of coverage at the time of execution of a contract, and resubmits it any time that insurance coverage, terms and conditions, or other information is changed or updated. Insurance requirements can be found in the contractor’s contract and VR-SFP chapters for specific services.

**…**

## 3.11 Documentation and Record Keeping

**…**

### 3.11.2 Record Storage

Contractors must keep their financial and supporting documents, statistical records, and any other records that are pertinent to the services for which a claim or report was submitted to the Texas Workforce Commission (TWC):

* safe;
* confidential; and
* available to TWC staff on request.

The records and documents must be kept as follows, whichever is later:

* For three years after the date that the final bill was submitted
* Until all billing-related questions are resolved

Contractors must report lost data within one business day to the:

* assigned contract manager and regional quality assurance specialist; or
* regional program support specialist.

#### Paper Record Storage

Paper is the preferred method for storing records.

Stored paper documents must be protected:

* as required in [3.3.4 Confidentiality](http://www.texasworkforce.org/standards-manual/vr-sfp-chapter-03" \l "s334); and
* in a retrievable and organized manner that prevents the documents from being stolen, tampered with, or damaged.

The contractor assumes all business risk associated with lost records. Lost records could result in adverse action against the contractor.

#### Electronic Storage (Not Cloud-Based or on a Third-Party Server)

Records stored on desktop computers or on portable devices (for example, on laptops, USB flash drives, hard drives, CDs, and DVDs) must be protected as required in [3.3.4 Confidentiality](http://www.texasworkforce.org/standards-manual/vr-sfp-chapter-03" \l "s334) and [3.3.5 Data Encryption](http://www.texasworkforce.org/standards-manual/vr-sfp-chapter-03" \l "s335).

Portable devices must be protected from theft, tampering, or damage. The contractor is responsible for all data collection and assumes all business risk associated with lost data. Lost data could result in adverse action against the contractor.

#### Cloud-Based Storage

Records that are stored entirely or partially in the cloud must be stored in compliance with the [Federal Risk and Authorization Management Program (FedRAMP)](https://www.fedramp.gov/" \t "_blank), or must be able to be made compliant in a short, defined period of time, as independently verified and validated by a FedRAMP-accredited [third-party assessment organization (3PAO)](https://marketplace.fedramp.gov/" \l "/assessors?sort=assessorName" \t "_blank).

The contractor must comply with TWC’s requirement that all data remain in the United States and meet TWC’s stringent privacy and security requirements.

TWC’s privacy and security requirements include the following:

* Protecting confidential TWC information, including personally identifiable information, from—at a minimum—unauthorized disclosure, unauthorized access, and misuse in accordance with the [National Institute of Standards and Technology’s (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)](https://csrc.nist.gov/publications/detail/sp/800-122/final), by establishing controls such as role-based access, encryption at rest, and encryption in transit
* Disposing of data in a manner that complies with [NIST Special Publication 800-88, Guidelines for Media Sanitization](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf" \t "_blank).
* Complying with TWC’s minimum encryption standards, that is, with the Federal Information Processing Standard (FIPS) 140-2, validated 256 bit, Advanced Encryption Standard (AES), and SHA-256 Cryptographic Hash Algorithm
* Complying with TWC’s minimum cryptographic protocol Transport Layer Security (TLS) 1.1 (TLS 1.2 preferred) for protecting the security and privacy of communications over a computer network, including over the internet
* Maintaining continuous process improvement and vigilance to assess risks, monitor and test security protection, and implement changes needed to protect TWC data
* Cooperating fully with TWC’s chief information security officer to detect and remediate vulnerability of the hosting infrastructure and/or the application
* Giving TWC access to the contractor’s facilities, installations, technical capabilities, operations, documentation, records, and databases, to the extent required to carry out FedRAMP assessments and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of the nonpublic TWC data that are collected and stored by the contractor

The contractor must notify TWC about new or unanticipated threats or hazards or about safeguards that cease to function, as the issues are discovered.

* Complying with any additional FedRAMP privacy requirements
* Understanding that TWC has the right to perform manual or automated audits, scans, reviews, or other inspections of the IT environment being used to provide or facilitate services for TWC

In accordance with Federal Acquisition Regulation 52.239-1, the contractor must do as follows:

* Obtain the contract officer’s written consent before publishing or disclosing the details of safeguards that the contractor designs, develops, or otherwise provides to TWC under contract (exception: disclosures to a consumer agency for the purposes of certifying or verifying authorization)
* Give TWC access within 72 hours to the contractor’s facilities, installations, technical capabilities, operations, documentation, records, and databases, to the extent required to conduct an inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of TWC data

Inspections include vulnerability scans of authenticated and unauthenticated:

* operating systems and networks;
* web applications; and
* database applications.

Automated scans can be performed by TWC personnel (or agents acting on behalf of TWC) using equipment operated or authorized by TWC and using TWC-specified tools.

* Notify TWC immediately, if new or unanticipated threats or hazards are discovered, or if safeguards cease to function

If the contractor chooses to run its own automated scans or audits, results from the scans or audits may, at TWC’s discretion, be accepted in lieu of vulnerability scans performed by TWC; however:

* the scanning tools and their configurations must be approved by TWC; and
* the complete results must be provided to TWC.

### 3.11.3 Record Retention

The contractor retains financial and supporting documents, statistical records, and any other records pertinent to the services provided under the contract for which a claim or report was submitted to TWC-VR.

Records and documents must be kept for three years after the final bill is submitted or until all billing-related questions are resolved, whichever is later.