



## INFORMATION SECURITY POLICY STATEMENT

### Purpose

This policy specifies the principles and requirements that Quiktrak has established to protect information assets owned by, leased, or entrusted to Quiktrak.

### Scope

This policy applies to all employees, vendors, independent contractors, and any parties who interact with, access, or store information assets owned by, leased, or entrusted to Quiktrak.

### Policy

Quiktrak is committed to protecting its information assets and shall act as a responsible conservator of information assets to which we are entrusted. Quiktrak will work toward achieving the following goals:

- Quiktrak shall comply with federal and state law, contractual obligations, and Quiktrak system policies related to information security.
- Quiktrak business processes shall be consistent with the above principles and, unless contrary to law, Quiktrak company policies or Quiktrak system policies shall follow the Quiktrak Information Security Management System (ISMS) standards and procedures for implementation.
- Quiktrak shall monitor and continually improve the ISMS through the achievement of specific objectives.

All Quiktrak leadership, employees, and relevant affiliates must actively support the above principles and are expected to take reasonable measures to protect information assets in their care.

### Enforcement

The ISO Integrated Management System (IMS) team, in cooperation with other Quiktrak authorities and administrators, will enforce this policy and establish standards, procedures, and protocols in support of the policy.

Any violation of the information security policy by a Quiktrak employee is considered “misconduct” under Quiktrak company policy. Additionally, violations of this policy may result in termination or suspension of access, in whole or in part, to Quiktrak information systems at the discretion of the ISO IMS team, whereby such action is deemed reasonable to protect Quiktrak or Quiktrak’s information infrastructure. Violations of law may also be referred for criminal or civil prosecution.

### Review

The VP of Technology and the COO/General Manager have approved the Information Security Policy Statement. The policy will be reviewed annually to ensure its continued suitability.

Rev: 6	Date: 5/31/2023	Doc. Number: IS-01
Title: Information Security Policy Statement		Approved By: Rob Murphy
Ref.: ISO 27001:2013 5.2		Page: 1 of 1