Information Security – Protecting LVVR Data

Confidentiality, Integrity, and Availability

A continuous chain of custody for the storage and handling of Locomotive Voice and Video Recording (LVVR) data requires technological safeguards and international accreditation for any virtual cloud storage provider. So how do you maintain confidentiality and integrity, yet make it available for inspection in a timely manner?

Safeguarding Your Data

Extensive testing assures security and provides ready access to the information needed to check regulatory compliance to privacy provisions collection, communication, preservation, access and use of LVVR data.

From edge to office, our onboard and back office systems go through rigorous testing to assure data remains true to its original version. Independent, third-party confirmation of Wi-Tronix SOC 2, Type 2 certification provides assurance that your data is maintained to the highest quality standards available in the industry today.

Data is recorded and made available to authorized users to better prepare investigators with immediate knowledge of the incident, while reducing inspection time, risk of liability, and eliminating the travel time in finding locomotives.

Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems that affect the ability to meet its objectives.

Availability. Information and systems are available for operation and use to meet objectives

Chain of Custody. Assurance that the Legal Department can prove the integrity of the ER and video data from a remote locomotive download to third party viewing

Integrity. The Certified Crash Hardened Memory Module and Power Hold Up feature eliminates worry of losing data in an incident or during power loss. Second-by-second monitoring of FRA data ensures data is recorded properly.

Preservation. Easy access to continuous second-by-second ER and connected system data history

Meeting Internationally Recognized Standards

- Systems securely leverage cellular networks and other features to ensure that endpoints are not accessible by other Internet users
- Systems are locked down to prevent malicious code from gaining a foothold
- Over-the-air security patches are promptly applied
- Data transmissions are encrypted
- Power Hold Up feature ensures the Violet Edge continues to function while Event Recorder data is sent to the Cloud, multiple seconds after power loss
- Data transferred to customers is encrypted and Single Sign On (SSO) is available
- Software supports full auditing and logging of customer activity
- VPN tunnels are used for business-to-business connections
- Incident response and disaster recovery procedures are defined, implemented, and periodically tested
- Code reviews
- Agile methods that include input from Information Security before feature development begins
- EN 50155:2017 Certified
- FRA Compliant for PTC & EATC
- SOC 2 Type 2

Find out what it takes to safeguard your data. Contact a Wi-Tronix expert to learn more at **marketing@wi-tronix.com**.

www2.Wi-Tronix.com