TULSA INSPECTION RESOURCES
INSPECTION & INTEGRITY

Cybersecurity & SAFE Technology

SAFE Technology Enhances Communications, Security, Safety, Compliance & Cost/Risk Management:

- GPS location, tracking, geofencing, alerts, speeding, and customized reports.
- US Government designed FirstNet proprietary 5G specialized network designed for first responders and critical infrastructure workers like TIR.
- Cybersecurity software loaded on a new, ruggedized smart phone, with push to talk capability & secure email.
- Multi-Factor Authentication (MFA) requirements to ensure that only authorized users and devices are accessing our collective systems.
- Safe and secure virtual desktop infrastructure to be used for all company/business related communication.

Microsoft

FIRSTNET
Built with AT&T

AT&T Workforce Manager

Key Drivers for Cybersecurity and SAFE Technology:

- Ensure remote field technicians can be reached at any time.
- FirstNet enhances communications for Safety stand-downs due to weather and other unanticipated events.
- Work force Manager GPS tracking reduces MVA's and aggressive driving risks.
- GPS data and Geofencing technology allows parties to confirm technician location, miles driven & per diem eligibility, etc.
- Reduce Cybersecurity threats from field technicians using personal, unprotected laptops and mobile phones for text and email.
- Use of TIR Secure Email instead of personal email and Virtual Desktop Interface ("VDI") for storage of project reports and documents in a secure cloud environment.
- Complex State and Federal privacy laws are growing, requiring the use of company owned devices instead of personal devices.
- FLSA litigation makes it important to truly know employees and contractor's location, and hours worked.
- Fortinet Phishing - Run monthly tests to ensure employees and field personnel are paying attention.

FIRSTNET
Built with AT&T

The FirstNet mission is to deploy, operate, maintain, and improve the first high-speed, nationwide wireless broadband network dedicated to public safety. This reliable, highly secure, interoperable, and innovative public safety communications platform will bring 21st century tools to public safety agencies and first responders, allowing them to get more information quickly and helping to make faster and better decisions.

Microsoft

Microsoft's Virtual Desktop Infrastructure (VDI) provides security at the highest level, featuring Data Loss Prevention, Multi Factor Authentication & Advanced Threat Protection. Paired with Microsoft's ONE DRIVE for storage of all business-related documentation, we maintain a safe and secure solution for company information. Mobile Field Employees access secure email and cloud storage to protect customer interactions.

Reliable and Safe Field Communication:

- Technicians carry a ruggedized FirstNet serviced Sonim mobile phone, delivering the nations most reliable data network and First Priority™ cellular service. We share the same network with first responders to keep the lines of communication open – when it matters most.
- Designed with heightened security to resist physical and cyber threats.
- Ruggedized to withstand power outages, and backed by a dynamic, highly trained disaster recovery organization.

AT&T Workforce Manager

Using the Manager App, administrators can access their Live View map and Users list on smartphones or tablets, directly from within AT&T Workforce Manager's mobile solution. This means that supervisors who are away from the office may still monitor the near real-time positions of their organization's employees.

With the Manager App, you can:

- Know field locations while on-the-go and keep field employees accountable.
- Shorten response times to critical customer situations.
- Stay up-to-date with near real-time activity updates.
- See how employees are dispersed in the field, from the field.
- Improve Safety Metrics by managing alerts and notifications to field employees in real-time.

Phishing Awareness and Training:

- The most vulnerable and primary means for data breach are phishing emails, thus we require our staff to successfully pass significant training and testing to identify phishing attempts.
- We provide a means to identify and report potential phishing attempts to our IT department.
- A recent study showed that 80% of breaches are caused by employee carelessness. At TIR, our constantly innovating training program requires that our team demonstrate awareness of scams, such as email attachments that contain malware or phishing emails.

5727 S. Lewis Avenue, Ste. 500 Tulsa, OK 74105
(877) 663-2977 | contactus@tirusa.com
www.tirusa.com