TD SYNNEX | *Public Sector*

Data Storage and Security for First Responders

Communications and data between first responders are considered "mission critical". The right information must get to the right person accurately, quickly, and it must be clear to understand. Bad actors want to hack into networks and lock up government computers with ransomware. This is a constant problem. If public safety agencies and local governments are not constantly improving their network security, they can be compromised. This is devastating to the agency. If hackers compromise a government network, it is possible that the private data of innocent citizens can be stolen. It is possible that digital evidence stored on servers can be destroyed or "tainted". The agency can be held responsible for any damages that occur.

Cybersecurity is a top priority today. The odds increase daily that an agency will be hit. Once hit, the chances of being hit again are even higher. We have the cybersecurity vendors and solutions that will enhance and protect the networks of public safety agencies. We have experts to assist in the design and implementation of the solutions. We can install them as well as finance them.

CIJS Requirements

The CJIS security policy includes security requirements, guidelines, and agreements reflecting the will of public safety agencies for protecting the sources, transmissions, storage, and generation of criminal justice information. CJIS Advanced Authentication policy requirements are required for all mobile systems including mobile data terminals and any other mobile devices that process National Crime Information Center access transactions.

Storage space

The amount of storage digital recordings require depends on:

- Number of cameras deployed
- Policy requirement for recording
- Retention requirements for the recordings
- Tagging, cataloging, and classifying data
- Controlling access
- Data security

FOR MORE INFORMATION

For ordering and questions, email:
rescue911@tdsynnex.com or **SLED@tdsynnex.com**