

Interoperable Communications Confidentiality Policy

1. Purpose:

The Confidentiality Policy is written to assure that DIS employees, including contractors, operating and maintaining public safety communications systems, hold information used or obtained in the course of their duties in strictest confidence.

2. Policy:

The responsibility for maintaining confidentiality of information lies with the individual or division entrusted with the information. Implicit in the trust is the expectation the individual will not divulge information, nor gain access to information unless there is necessity based on the job description or standards of practice.

Access to the computer systems and proprietary data (including, but not limited to research, system operational data (such as talkgroup information, tower locations, frequency information), Agency information and employee data) is determined by job responsibilities of the individual seeking access and is to be controlled and monitored through management oversight and identification authentication practices. Access to computer information systems is to be controlled at a minimum, by the use of individualized and confidential user sign-on and password codes. DIS employees operating and maintaining public safety communications systems will be issued confidential and individualized sign-on codes.

Federal and State laws addressing confidentiality of data as well as the policies and regulations of oversight and accreditation agencies will be observed. It is the responsibility of managers to ensure that staff is adequately informed about relevant laws and regulations.

DIS employees and contractors operating and maintaining public safety communications systems must sign a Confidentiality Agreement which acknowledges their commitment to protect and maintain the confidentiality of all DIS, employee, and Agency information, and all proprietary information to which they have access or have gained access in the course of their work.

Signing the Confidentiality Agreement attests the person understands the consequences of violating the agreement.

3. Controls:

The consequences of violating the Confidentiality Policy may result in discipline up to and including immediate termination. Violation of confidentiality may also create civil and criminal liability.