RadioAudit

Automates the process of radio audits, making compliance efficient, fast and accurate

Regular auditing of TETRA radios to verify both the device owner and the radio's security status is a necessary part of keeping communications secure. **RadioAudit** is a data application that **simplifies** and **automates** the auditing process, reducing manual handling and delivering **accurate** reports to fleet administrators

COMPLETE ACCURATE AUDITS AND MINIMISE RISK OF RECORDING ERRORS

- Audits can be completed automatically, significantly reducing administrative burden, and allowing additional or follow-up audits to be run as required
- Built-in reminders and easy data input for radio users ensures high response rate
- Allows efficient management of the radio fleet, confirming security compliance and meeting regulatory requirements

sepura

Going further in critical communications

RADIO AND CONTROL ROOM APPS

SIMPLE, EFFECTIVE DEPLOYMENT TO ENHANCE AUDITING PROCESS

- Automated auditing is scalable to fleet size and across multiple Sepura radio models, completed remotely by the radio user
- Auditing is controlled by a PC/server application. Fleet data can easily be imported using information from Sepura Radio Manager to allow fast initial deployment
- Audits are executed by each radio user via an application on the radio. Sepura Radio Manager handles the simple installation process

AUTOMATED PROCESS

- Audits can be initiated by a fleet administrator to authenticate each radio holder within the fleet
- The audit prompts radio users to enter a password to prove they are the legitimate holder of the radio
- Built-in data analytics tools enables viewing and querying of collected audit data, with the option to export to Excel
- Automatically generated audit reports are presented clearly for further analysis, reducing the burden on administrative teams

TECHNICAL SPECIFICATIONS

SERVER APPLICATION

Minimum Hardware requirements:
- 64-bit PC Server, 3GHz+ CPU, 8GB memory, 256GB disk space (SSD or RAID recommended)

Operating System
- Windows Server 2016 or later or Windows 10 Pro
- Supports clustered installation for redundancy

Requires Sepura SCG22 or SRG3900 for PEI connection to the TETRA network
SDS message sending is staggered to ensure negligible imact on network loading
Audits can be scheduled to run on a timed basis (eg every six months) or initiated manually
Audit reports will show:
- Radios with valid users
- Radios with valid users but compromised tamper seals
- Radios showing no response or invalid user

Minimum Data Captured by Reports: Date/Time, ISSI, Tamper Seal Status, User ID, User ID Validity
Optional Data Integration with 3rd Party application Via REST API

RADIO APPS

Compatible with the following radios:
Handheld:
- Sepura SRH and STP Series using V10.13 Firmware or later
- Sepura SC Series using V2.0 Firmware or later

Mobile:
- Sepura SRG using V10.13 Firmware or later
- Sepura SCG using V3.1 Firmware or later

sepura

For a full list of offices and distributors or any other information, visit **sepura.com**

0141_0521_V6