El Dorado County
Emergency Services Authority

Policy Subject Matter: **Security Policy**
Review Date:
Revision Date:
Creation Date: **03.02.11**

I. Policy:
JPA member agencies and their employees shall utilize the security measures that have been implemented to secure vehicles and equipment.

II. Purpose:
To provide direction on the use of security measures that will enhance the ability to safeguard vehicles and equipment from theft and vandalism.

III. Procedure:
Effective security measures begin with each employee being aware of their surroundings, practicing good crime prevention techniques, and utilizing the security systems the JPA has implemented.

A. Situational Awareness
Because crimes of theft and vandalism can occur in any setting and under a multitude of circumstances, it is important to never let your guard down. While on duty:
1. Be aware of your surroundings and consider the history of criminal activity in the area.
2. Be on alert for indicators that a threat exists.
3. React to eliminate those threats by reporting suspicious people to law enforcement, utilizing the medic units locking systems and when possible park in illuminated area.

B. Crime Prevention Techniques
Criminals are often drawn to those favorable opportunities and situations where they can commit a crime and avoid detection and capture. Some proven strategies for deterring crime include:
1. Do not leave vehicle doors unlocked and open with expensive equipment visible.
2. Avoid leaving vehicles and equipment unattended.
3. Call for assistance (Fire-Police-Sheriff) when needed to stand guard.
4. Safeguard vehicle ignition keys and cabinet keys.

C. Security Measures

The JPA has installed an electronic anti-theft security system on the ambulances in the JPA fleet. For the system to work in an effective manner and serve its purpose, employees shall:

1. Check the security system at the beginning of each shift to insure it is functioning properly.
2. Utilize the system at all times unless circumstances dictate otherwise.
3. Instruct all new employees on how to use the system.
4. Keep the system details and password confidential.
5. Do not disable anti-virus software.
6. Do not change or modify technical applications from its agency authorized configuration.
7. Maintain security and confidentiality of personal identification numbers when issued.

Marty Hackett
Executive Director