Allied Radio Matrix for Emergency Response (ARMER)
Standards, Protocols, Procedures

Document Section 4	**Maintenance**	**Status:** Complete
State Standard Number	**4.11.0**	
Standard Title	**Computer Access to the ARMER Network**	
Date Established	**7/11/2006**	**SRB Approval**: 7/27/2006
Replaces Document Dated		
Date Revised		

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures of remote computer access to the ARMER system for maintenance and support purposes, including:

- System Administrative Management
- Technical support and problem solving
- Call duty

2. Technical Background

- **Capabilities**

Using an Internet Protocol (IP) based Keyboard-Video-Mouse (KVM), technology provides the following advantages:

- Any computer can be used for remote access
- High speed connections are possible through the internet and office network
- The ARMER network remains completely isolated
- Access is controlled and managed by individual agencies
- Some IP-KVMs also support dial-in capabilities as fallback protections

- **Constraints**

Issues with previous methods of remote access:

- Dial-in access was problematic and slow
- Required a clean, dedicated computer
- Added risk by potentially introducing hazards from the remote computer

Issues with using an IP-KVM remote access solution:

- Increased cost of roughly $1,000 for the IP-KVM
- May require coordination with office network management staff
- Remote mouse control can be tricky, with rapidly changing graphics

3. Operational Context

In order to protect and isolate the network of the ARMER system, connections for remote access will not be allowed to directly connect to the ARMER network or computers.

In order to meet the remote access needs for the maintenance and support of the system, an intermediate device will be utilized, commonly referred to as an IP-KVM. The network interface of the KVM will be connected to the agency office network, and the keyboard-video interfaces will be connected to a management client on the ARMER network. This provides remote access capability while simultaneously providing complete network isolation and protection.

Any computers used to connect to the ARMER network directly will be clean, dedicated computers for the purpose of supporting the ARMER system and will not be used on any other networks. This prevents introducing anything hazardous to the ARMER network from other networks or the internet.

4. Recommended Protocol/ Standard

Direct remote access to the ARMER system network and computers is not permitted.

Remote access to the ARMER network will be accomplished by using an IP based KVM.

Any computers used to connect to the ARMER network directly will be clean, dedicated computers for the purpose of supporting the ARMER system. The ARMER system does have a supported anti-virus server, and it should be encouraged that dedicated service computers be set up with accounts on the anti-virus server for automatic updates.

5. Recommended Procedure

IP-KVM installations would require approval of the Statewide System Administrator.

The network interface of the IP-KVM will be connected to the agency office network and not directly to the internet. This adds an additional security layer the office network provides.

The KVM interface of the IP-KVM will be connected to an ARMER System Manager client owned by the agency installing the IP-KVM.

The IP-KVM will be capable of and configured to use:

- Password protection
- HTTPS “SSL” Secure Socket Layer communication

The IP-KVM will use an agency secure password defined by:

- Minimum of 8 characters
- No English words or known passwords
- Containing alpha, numeric, and non-alphanumeric characters

System Management clients with an IP-KVM installed will be configured with a screensaver password protection set at a maximum of thirty (30) minutes.

6. Management

The System Administrators will be responsible for managing remote access to the ARMER system.