|  |
| --- |
| ***REPLACE WITH YOUR MASTHEAD*** |
| **VFIS logo black JPG** | **SOG Title:** |
| **SOG Number:** |
| **Original Date:** | **Revision Date:** |
| **ABC Fire Department General Operating Guideline** |

**Data Security for Emergency Communications Centers**

***This is a sample of a standard operating guideline (SOG) on this topic. You should review the content, modify as appropriate for your organization, have it reviewed by your leadership team and if appropriate your legal counsel. Once adopted, make sure the SOG is communicated to members, implemented and performance monitored for effective implementation.***

**Purpose:**

To establish a procedure to manage data security at emergency communication centers.

**Procedure:**

Technology has revolutionized every aspect of our lives, including emergency communications. Modern communication systems and computer networks are custom designed for specific industries. Their operation may require the exchange of digital data across platforms including servers, microwave systems and on and off-site (cloud) data storage mediums. While some of the information contained in these systems is public record, there are still security concerns. Breaches can affect the computer aided dispatch (CAD) system, geographic information (GIS) mapping system and the radio network. Data security breaches could be part of some type of criminal activity or cyber-attack or be a by-product of another network breach. The risk is the intentional or unintentional interruption of service that may not be discovered until system reliability is compromised.

To help lessen the risk of a breach, consider developing a data/information technology (IT) security plan in conjunction with system partners. This may include the Telephone System Company provider, GIS provider, CAD vendor, Internet vendor and the communications/radio vendor.

* The plan may address:
* Assigning a responsible person for security functions.
* Training and educating employees that have access to data systems.
* Establishing policies to limit or restrict personal use of computer equipment.
* Physical security measures at equipment rooms and remote server sites.
* Network security for all IP based systems.
* Provisions to help prevent cyber-attacks on the center’s computers and servers.
* Plans to update operating and security software periodically, including secondary public safety answering points (PSAP) locations or emergency operating sites.
* A written policy to address or investigate suspicious activity or complaints.
* Periodic auditing of the total IT security system.

***This is a sample guideline furnished to you by VFIS. Your organization should review this guideline and make the necessary modifications to meet your organization’s needs. The intent of this guideline is to assist you in reducing exposure to the risk of injury, harm or damage to personnel, property and the general public. For additional information on this topic, contact your VFIS Risk Control representative.***

**References:**

VFIS Communique – “Data Security for Emergency Communications Centers”