

|  | <b>Standard Operating Procedure</b>                         |                            |                        |
|---|---|----------------------------|------------------------|
|   | Title / Subject<br><b><u>Building and Site Security</u></b> | Effective Date<br>07/14/15 | Revision Date<br>----- |
|   | <u>References/Updates:</u>                                  |                            |                        |

**Contents:**

|    |              |        |
|----|--------------|--------|
| 1. | Introduction | Page 1 |
| 2. | Purpose      | Page 1 |
| 3. | Definitions  | Page 1 |
| 4. | Scope        | Page 2 |
| 5. | Policy       | Page 2 |
| 6. | Procedures   | Page 4 |

**1. Introduction:**

The Statewide Interoperability Executive Committee (SIEC) has determined the need to establish a standard procedure for the security of the Statewide Interoperable Radio Network (SIRN). This SOP will define the standards needed to safeguard the system. In order to protect the security and integrity of the network, this security procedure is necessary.

**2. Purpose:**

The security and integrity of the SIRN is of the utmost importance. Therefore, the SIEC is implementing this SOP to aid in the guidance for the security of communication buildings and sites housing SIRN equipment.

**3. Definitions:**

**Authorized Person** – Any person that has a need to access a SIRN site for approved and authorized work and/or maintenance. This person meets the requirements of this procedure pertaining to background checks.

**Building** – Physical structure that houses the electronics equipment pertaining to the SIRN, Microwave System(s) or other associated equipment. This may actually refer to multiple buildings within one site.

**Compound** – The location inside the fence that houses the building, tower, generator, tanks, etc.

**Government Employee** – Any person that is employed (not contracted, hired or volunteering for) by any Federal, State, County or Local entity that has a valid need to enter the sites of SIRN.

**Site** – Physical location, including the building, tower and compound, generally referring to the area inside the fenced area at each site.

**Tower** – The radio tower, ice bridge and associated components.

**Unfavorable Background Results** – A background check that is returned with any Felonies, Larcenies or any convictions for tampering with communications shall be considered as unfavorable.

**Vendor** – Refers to any person, organization or other entity that is not employed by a government entity. This could include for profit, on a volunteer basis or otherwise provide services or installations at the site.

*Additional definitions and acronyms can be found on the SIRN website at <http://www.sirn.wv.gov>.*

#### **4. Scope:**

The scope of this SOP includes any building or site in which SIRN equipment is located, and is to include:

- Physical site access
- Physical building access
- Building use restrictions
- Vendor access
- Reporting of access to sites
- Standards used to evaluate the access

#### **5. Policy:**

##### **5.1. Physical site access**

- 5.1.1. Each site shall be kept locked in a manner that would prevent unauthorized access, including but not limited to locks on all fences, gates and buildings.
- 5.1.2. Only authorized persons may have access to the site per this guideline or by emergency permission given by the SWIC, SIRN Tech, RIC Chairman or the Director of DHSEM.

5.2. Physical building access

- 5.2.1. Each building shall be kept locked in a manner that would prevent unauthorized access, including but not limited to deadbolt style locks on all doors.
- 5.2.2. Access to the buildings shall be restricted to necessary and authorized persons to perform maintenance, installation or other officially approved work.

5.3. Building Use

- 5.3.1. Buildings containing SIRN equipment should be restricted to Public Safety and/or Government Use Only unless otherwise approved by the building owner and the SIEC.
  - a. Terms and Conditions of any collocation agreement will set forth access and responsibilities for access.

5.4. Vendor Access

- 5.4.1. Any vendor requesting access to any site or building must have on file with the SWIC an acceptable background check.
  - a. Should anyone receiving Unfavorable Results on their background check wish to have their status reconsidered that person may submit in writing the request, explanations and other supporting documents to the SWIC for review and presentation to the SIEC for final review.
- 5.4.2. The SWIC shall prepare and maintain a list of approved persons that have successfully passed a background check.
  - a. All persons of a “Work Crew” must meet this requirement, not just a single person.
- 5.4.3. Keys shall be granted to vendors only for the timeframe to complete the work agreed upon and once the requirements of this guideline are met.
  - a. Vendors shall not be assigned keys
  - b. Records shall be kept by key holders as to which vendor, name of person, time, date and work to be performed by anyone granting keys.
  - c. No key shall be copied by a vendor.
  - d. Keys shall not be kept overnight by vendors.

- 5.4.4. Violation of these provisions will result in permanent removal from the approved site access list.
- 5.5. Governmental Employees shall be exempt from this section should their employment require access to sites and/or buildings and the employer requires background checks meeting the requirements of this policy.

## 6. Procedures

### 6.1. Reporting Access

- 6.1.1. All entry to sites and/or buildings shall be reported before such entry and upon exit to a location determined by the SIEC.
  - a. This location shall be available 24 hours per day, 7 days per week.
  - b. This location shall keep records of access reports.
  - c. This location shall check the status of crews on site periodically to ensure safety of the workers as deemed necessary.
    - 1. When reporting access to a site, the call center should note if the person or crew will need checked on and work out the particular times and methods for checks.
- 6.1.2. The current location to report entry/exit.
  - a. Primary: Medical Command – Flatwoods
  - b. Secondary: WVDHSEM – Call Center
- 6.1.3. The notifications can be made by:
  - a. SIRN Radio using the TECH 1 Talkgroup (See General Programming Procedure for use of this Talkgroup), or
  - b. Telephone 1-866-767-2346 (Primary), 304-558-5380 (Secondary)

### 6.2. Implementation

- 6.2.1. Those desiring site access and not covered under other provisions of this procedure shall have 90 days to be in compliance with this guideline.
- 6.2.2. To facilitate the implementation of this SOP, the WV State Police will perform the background checks for the first 90 days, after which a private firm must be used with results being forwarded to the SWIC.

- 6.2.3. Should a person be an approved active programmer for the SIRN, that background check will be accepted.
- 6.2.4. All background checks, rechecks and companies used for checks must follow the current CJS policy.
  - a. Any questions regarding the acceptance of a background check should be forwarded to the SWIC.
  - b. For vendors that operate in multiple counties only a single background check is needed, not one for each county.

### 6.3. Exemptions

- 6.3.1. The SIEC may, for special circumstances, grant an exemption to certain parts of this procedure.
  - a. To apply for an exemption, a request must be made in writing to the SWIC, giving in-depth details of the reason for the exemption.
- 6.3.2. On sites with multiple buildings, towers, etc. this policy shall only apply to facilities that affect SIRN.
- 6.3.3. Persons delivering fuel, mowing grass or other activities that does not involve entering the building, opening the enclosures on any generator or building or performing any work on towers shall not have to have a background check.
- 6.3.4. If an entity has a site access policy that exceeds the provisions of this document, that agency may operate under the more strict guidelines.
- 6.3.5. The SWIC, RIC Chairperson or SIRN Tech may, in an emergency situation, grant supervised access to sites.