Standard Operating Procedure

Title / Subject

Site Security

References/Updates:
Updated: 12/11/2023

1. **Introduction/Purpose**
   This policy is pertinent to any agency that utilizes the WV SIRN. Its purpose is to comply with all Federal NIMS Guidelines.

2. **Definitions**
   All definitions are located in the "Definitions" document located on the SIRN Website at www.sirn.wv.gov.

3. **SIRN Site Security**
   - **a.** Physical site access
     - **i.** 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.
   - **b.** Physical building access
     - **i.** 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.
     - **ii.** Access to the buildings shall be restricted to necessary and authorized persons to perform maintenance, installation or other officially approved work.
     - **iii.** Amateur radio operators and equipment shall not be located in SIRN equipment buildings.
   - **c.** Building Use
     - **i.** 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.
     - **ii.** Non-state owners of buildings that have SIRN equipment inside should be considerate of those who enter the building.
   - **d.** Vendor Access
     - **i.** Any vendor requesting access to any site or building must have on an acceptable background check.
       1. Should anyone receiving Unfavorable Results on their background check wish to have their status reconsidered that person may submit in writing the request to the SIEC for final review.
     - **ii.** All persons of a "Work Crew" must meet this requirement, not just a single person.
     - **iii.** 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.

iv. Vendors shall not be assigned keys.

v. Records shall be kept by key holders as to which vendor, name of person, time, date and work to be performed by anyone granted keys.

vi. No key shall be copied by a vendor.

vii. Keys shall not be kept overnight by vendors.

viii. Violation of these provisions will result in permanent removal from the approved site access list.

ix. The copying of or loss of an issued key may result in the vendor being responsible for replacement key(s) and/or rekeying of the site locks.

x. 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.

xi. For vendors that operate in multiple counties only a single background check is needed, not one for each county.

e. Reporting Access

i. All entry to sites and/or buildings shall be reported to the State Watch Center at 304-558-5380 before such entry and upon exit.

ii. 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.

f. All background checks, rechecks and companies used for checks must follow the current CJIS policy.

g. The SIEC may, for special circumstances, grant an exemption to certain parts of this procedure.

h. On sites with multiple buildings, towers, etc. this policy shall only apply to facilities that affect the SIRN.

i. 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.

j. If an entity has a site access policy that exceeds the provisions of this document, that agency may operate under the stricter guidelines.