Saint Louis COUNTY
EMERGENCY COMMUNICATIONS COMMISSION

Policy 18-18 **September 13, 2018**

ECC Site Security Policy

I. PURPOSE

The protocols authorized by this policy will focus only on the physical security of and access to infrastructure and equipment of systems under the control of the St. Louis County Emergency Communications Commission (ECC).

II. GENERAL

The ECC provides systems; including 9-1-1, outdoor warning siren, and radio communications system, critical to the safety of the citizens of St. Louis County and vital for first responders to perform their mission. Security measures are required to protect the operational integrity of the ECC's systems from the malicious intent of interrupting, altering, or destroying the systems intended functional capabilities.

Security requires multiple layers of physical, procedural, and technical protections; together the multiple layers of security create a comprehensive strategy to increase the level of security to ECC Systems.

III. DEFINITIONS

ECC Systems – All systems under the control of the ECC including but not limited to outdoor warning sirens, Next Generation 9-1-1, and SLATER.

ECC Sites – The physical location of ECC infrastructure and equipment including, but not limited to, radio tower sites, data centers, PSAPs, and sirens.

Field Services Manager – A member of the ECC staff who is responsible for managing ECC building and infrastructure systems.

Personnel – Includes all persons assigned to perform services on ECC infrastructure and equipment including ECC Staff, manufacturers, vendors, and contractors.

SLATER – The ECC owns and operates the St. Louis Area Trunked Emergency Radio (SLATER) system, an 800 MHz P-25 Digital Trunked Simulcast Radio System, licensed by

the Federal Communications Commission (FCC) which provides county-wide and regional interoperable radio coverage for public safety agencies within St. Louis County.

IV. POLICY

A. The ECC has sole authority to grant, deny, or revoke access of any person(s) to ECC Sites.

B. This policy applies to all persons who request or have been granted unsupervised access to any ECC Site.

C. Site security information and technical system details which could compromise site security may be closed records under Chapter 610 RSMo. Such information shall not be shared without the prior written authorization of the ECC Director.

D. Keys, access cards, and combination lock codes of ECC Sites will be under the control of the ECC and only distributed to Personnel authorized to have access necessary to perform their assigned duties or services.

E. The ECC shall implement any and all measures for ECC Site security protection, including but not limited to access restriction techniques, barriers, sensors, alarms, cameras, and other deterrent and detection devices.

F. All Personnel assigned to perform services on ECC equipment, infrastructure and systems shall report acts in violation of this policy to the ECC Director.

V. PROCEDURE

A. ECC Site access grant requests shall be made via email to the ECC Director. Prior to granting authorization, all Personnel must:

1. Provide a police record check through St. Louis County Police Department's Record Division for the individual to be granted access.

2. The ECC Director and St. Louis County Police Department shall review the record checks and shall determine whether to grant access to ECC facilities.

3. Failure of the contractor or vendor to ensure that this section is complied with shall be considered a breach of security and will result in the removal of any and all contract employees that are not in compliance with this section.

4. The St. Louis County Police Security will perform follow up police record checks on all contractor and vendor employees annually.
5. Unsupervised access requires the written authorization in advance by the ECC Director.

B. Keys, access badges, and combination locks will be managed by the Field Services Manager of the ECC. An annual audit will be performed on the ECC Site access list of persons with unsupervised access rights.

C. Sharing or loaning access badges, lock combinations and keys is not permitted. Vendor service providers may request temporary access from the ECC Director in writing. No access will be authorized prior to written authorization from the ECC Director.

D. Personnel at secure facilities must have appropriate badges/or access authorization material displayed in plain view at all times.

E. Personnel who are no longer employed or perform duties supporting the ECC, shall return all keys and access cards to the ECC immediately. ECC vendors and contractors shall notify the ECC of any personnel changes impacting access to ECC sites.

F. Notifications of urgent staff issues, such as discharged employees or cancelled vendor contracts, shall be immediately communicated by email to the other system administrators of neighboring radio systems.

G. Persons without authorized access must be escorted by ECC staff or designee on the premises at all times.

H. All equipment cabinets, doors, and gates must be closed immediately upon the conclusion of work activities and prior to exiting the facility.

I. Site combination locks shall be changed every 6 months. Changes to the combination code shall be distributed to all Personnel with authorized access.

J. Any security breaches, or suspected evidence thereof, shall be reported to local authorities and the ECC Director.

VI. SITE SPECIFIC SECURITY

A. Radio Tower Sites

1. All personnel visiting a radio tower site must log the purpose of their visit on the site log form affixed to the interior of the shelter.

2. For visitation after-hours (17:00 – 07:00 hours), all Personnel shall report to the Motorola Network Operation Center (NOC) immediately upon entry and at the conclusion of the visit, following the instructions posted

inside the shelter. The NOC will notify Wireless USA of all after-hours access at the time the request in made. The NOC will contact Wireless USA to respond for entry alarms which are reported after hours. The Wireless USA staff member responding to the entry alarm will notify ECC Personnel at the time they receive notification of the entry alarm.

3. All Personnel, excluding ECC staff, shall inform the appropriate ECC staff member; i.e. Radio Service, Network or Field Services manager, of all visits to radio tower sites prior to arrival during business hours.

B. Data Centers

1. Access to the Ohlendorf ECC Data Center and the County-Wide Backup at Ladue Bluffs will be managed by ECC staff. Entry will be limited to authorized personnel required for the operation and maintenance of the systems housed in the data center.

2. Visitor badges specific to Ohlendorf ECC Data Center entry shall be kept with building security. Security personnel will obtain authorization from ECC staff prior to assignment of data center badges at Ohlendorf and shall monitor camera footage of the data center for suspicious activity.

3. Cabinets in the ECC Data Center will be keyed in accordance to their function in one of the five categories: Radio, 9-1-1, OEM, County IT, and General. Keys will be distributed to authorized personnel of those operational units by the ECC Director.

4. Commercial data center facilities have strict building access procedures requiring an Access/ID Card. Access to ECC owned equipment in commercial or private data center facilities shall require prior authorization by the ECC Director.

   a. The ECC Director and GDIT Project Manager have authority to coordinate with Digital Reality Trust (DRT) Management Office to authorize personnel to gain access to ECC Equipment.

   b. The ECC Director is responsible for managing access cards and keys to ECC equipment at the DRT facility.

C. PSAPs (ECC Equipment Only)

1. ECC equipment housed at PSAPs shall remain in controlled access areas and shall be clearly marked with ownership and ECC contact information.

2. Only ECC staff or its designee(s) may adjust, alter, modify, move, or perform maintenance activities on ECC equipment.

3. Site access shall not be unreasonably denied to Personnel that would interfere with their system maintenance responsibilities.

D. Sirens

1. Agencies and/or public service utilities with authorized equipment attached to Outdoor Weather Warning Sirens poles are required to notify the ECC Field Services Manager in writing prior to performing any installation, maintenance or upgrades to their physical assets.

VII. Security Acknowledgement

All non-ECC Personnel shall review the policy, complete the acknowledgement page and return to the ECC Director in order to receive authorization for unsupervised access to ECC Sites. Re-acknowledgement may be necessary upon amendments of this policy.

VIII. MEMORANDUM of UNDERSTANDING

This policy is covered under the MOU signed previously by each public safety user and outside agency user on the SLATER system.

Approved by the Emergency Communications Commission on 9/13/18

Director,
Emergency Communications Network

Chairman,
Emergency Communications Commission

ECC Site Security Policy #18-18
Acknowledgement

I, _____ agree to abide by the security measures set forth in the Site Security Policy and in this acknowledgement and understand actions in violation may result in revocation of access privileges to ECC System Sites.

(Please Initial Each)

_____ I agree I will not distribute system design information and technical details on ECC sites and systems.

_____ I agree not to share or loan keys, access badges, and combination codes.

_____ I agree to have appropriate badges or access authorization material displayed in plain view at all times.

_____ I agree to return all access badges, keys, and ECC owned equipment, tools, and material immediately upon reassignment or separation of employment where I no longer support the ECC.

_____ I agree to record the purpose of site visits into site logs and provide the proper notification(s) as directed by the ECC.

_____ I agree to maintain physical security of ECC Sites by closing and locking all gates and doors at the conclusion of each site visit.

_____ I agree to report acts in violation of this policy to the ECC Director.

_____
Signature

_____
Print Name

_____
Title

_____
Company

_____
Date