NSTCINST 5230.2
N00
17 Mar 16

NSTC INSTRUCTION 5230.2

From: Commander, Naval Service Training Command

Subj: NSTC INFORMATION TECHNOLOGY SERVER CABINET KEY MANAGEMENT
       PROGRAM

Encl: (1) Sample Access List

1. <u>Purpose</u>. This instruction implements the Naval Service
Training Command (NSTC) policy for the management of keys used
to access cabinets containing servers connected to authorized
legacy networks supported by NSTC N6.

2. <u>Applicability and Scope</u>. This instruction applies to all
NSTC members and contractors who are authorized access to
cabinets containing servers connected to authorized legacy
networks supported by NSTC N6.

3. <u>Exceptions</u>. Keys to communications closets are held by
watch standers in accordance with local command policy.

4. <u>Definitions</u>

    a. <u>Communications Closet</u>. A closet or small room in a
building in which communications (e.g., computer network,
telephone) equipment is located.

    b. <u>Key</u>. A key may be a physical key or a combination used
to open a locked container.

    c. <u>Key custodian</u>. A person who is authorized to possess a
key covered by this instruction.

    d. <u>Key locker</u>. A wall or table-mounted, lockable cabinet
used for securing keys.

    e. <u>Server cabinet</u>. A lockable cabinet usually located
within a communications closet, which contains a server, switch,
router, or other network asset.

    f. <u>Server Cabinet Key</u>. A key to a server cabinet.

5. Policy. The following policies apply to server cabinet keys at NSTC:

    a. Access to cabinet keys is a form of privileged access. Accordingly, only NSTC N6 members and contractors who are members of the Cyber Security Work Force (CSWF) and are current with all CSWF certification and training requirements are authorized access to cabinet servers and keys.

    b. Server keys will be maintained in a key locker. The number and location of key lockers will be designated by NSTC N62 Operations and Infrastructure Manager.

    c. An authorized access list will be maintained in every key locker, signed by the NSTC N6 Department Head, reviewed quarterly and updated as needed.

    d. Custodians for key lockers will be designated in writing by the NSTC N6 Department Head. No more than two custodians will be designated for each key locker. The NSTC N62 Operations and Infrastructure Manager shall retain an extra key/combination. Letters of designation shall be maintained by the NSTC N62.

    e. Server cabinet keys will be signed out and signed in by the custodian of the key locker from which the key is obtained. The sign in/out list or logbook will be maintained in the key locker. All keys shall be accounted for at all times, either signed in and present in the locker or signed out.

    f. Lost key procedure. A lost key shall be reported immediately to the supervisor.

    g. Cabinets shall be locked at all times when not being accessed for authorized server work. Work on a server is only authorized through a REMEDY ticket or in an emergent situation (e.g., server is smoking). A cabinet that is found unlocked shall be reported immediately to the supervisor.

    h. Keys may be retained by authorized personnel and do not have to be checked in and out each day. Key holders shall produce any key checked out to them at any time when requested by proper authority (i.e., contract Task Lead, contract Technical Advisor, or NSTC N6A Information System Security Manager). Only one key of each cabinet type may be held by an authorized person at any time.

i.   Server cabinet key holders shall be designated in writing by the NSTC N6 Department Head.

j.   The NSTC N62 shall inventory keys once per quarter.

k.   Anyone who is found to have a key other than in accordance with this instruction is subject to disciplinary action up to and including loss of privileged access, removal from the CSWF, or removal from federal or contractor service.

6. Responsibilities. The NSTC N62 Operations and Infrastructure Manager is responsible for the Server Key Control Program.
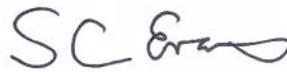
S. C. EVANS

Sample Access List

DD Mmm YY

MEMORANDUM FOR THE RECORD

Subj: ACCESS AUTHORIZATION FOR NSTC TRANET-U KEY LOCKERS

1. The following technical personnel are authorized access to
all TRANET_U Key Lockers:

Smith, William   Jones, Adam
Baker, Sue   Carson, Jennifer
Roberts, Michael

2. The personnel listed above are authorized to check out
temporary issue keys with a logbook entry, including key number,
checkout date/time, name and signature of recipient, return
date/time, and signature of the person receiving the returned
key.

                              A. B. ADAMS
                              N6