Minnesota Department of Corrections

Policy Number:	**301.060**
Title:	**Access Control Devices**
Effective Date:	**11/5/19**

PURPOSE: To assist facility security and provide for the systematic control of keys and other access and securement credentials and devices. Each facility must maintain safe and secure methods for the issue, distribution, maintenance, control, and accountability of keys and other access control credentials and devices

APPLICABILITY: All facilities and programs

DEFINITIONS:
Access control credentials – included physical (keys, radio frequency identification (RFID) tags, key fobs, smart devices, biometrics, etc.) and logical (cypher lock personal identification numbers (PINs), passwords, etc.) form factors which, upon authentication, may secure physical barriers or grant passage at physical barriers; they may also limit or refuse access if invalid credentials are presented.

Access control devices – includes all system equipment including door position switches, controllers, and wiring; administrative software; mechanical and electronic barrier, door, gate, or actuator locks or locking devices; vehicle door locks and ignition switches; building environmental and power management locks or controls; elevator and other ingress or egress points; and any and all access to secure areas and vehicles.

Employee-retained keys – keys issued by the facility to store personal items or to access personal use areas (examples include: cell phone lockers, mailboxes, workout areas, or other areas as designated).

Secured key ring – tamper-proof ring that does not allow the addition or removal of keys without breaking the ring.

PROCEDURES:
A. Each facility must provide comprehensive and effective control of access control credentials and devices, including procedures regarding the following:
   1. Issuing access control credentials and devices. (Facility master keys are only issued on a limited basis, as absolutely necessary, and the facility must annually review its roster of master key holders for appropriateness.);
   2. Inventory of access control credentials and devices;
   3. Handling of access control credentials or devices by employees, contractors, volunteers, and interns;
   4. Designating one position as the primary person responsible for access control procedures;
   5. Lost or damaged access control credentials or devices;
   6. Recording access control credentials and devices;
   7. Storing access control credentials and devices, including:
      a) Access control credentials and devices are stored in assigned key cabinets and are cross-indexed; and
      b) Color or other coded emergency and restricted access control credentials or devices are stored in separate, secured locations;
   8. Reporting methods for access control credentials and devices;

9. Inventory and maintenance checks;
10. Staff training or orientation specific to access control equipment and procedures;
11. Means for the immediate release of offenders from locked areas during an emergency, including a backup mechanical release method in the event of power failure or malfunction; emergency keys must be tested and rotated regularly to ensure effectiveness, with documentation of the testing;
12. Procedures that may be employed in areas where the loss of keys to offenders could result in a serious security breach and the potential loss of control of an area of the facility; and
13. Designation of staff persons whose primary responsibilities include granting access to certain areas via key care, ID card, or biometric devices.

B. General access control credential and device regulations

1. The access control officer assigns key rings based solely on the business need of staff as designated by the appointing authority. The access control officer tracks the keys on all key rings assigned to staff or to areas, ensuring access is restricted to approved areas.

2. Handling access control credentials, devices and locks

a) Staff must maintain strict physical control of access control credentials and devices at all times.

(1) Maximum security access control devices (such as Mogul® or Folger-Adam® type devices) must never be displayed or left hanging from or tucked into belts.

(2) Access control credentials and devices must be handled in such a manner as to prevent them from being dropped. Access control credentials and devices are passed hand-to-hand and must never be thrown from one staff person to another, left on desks or in desk drawers, or left hanging in a lock. Staff may use key keepers to facilitate physical control of keys.

(3) Offenders must never handle security access control credentials or devices. Staff must handle access control credentials and devices in such a way that offenders do not have the opportunity to examine them.

(4) To prevent offenders from learning access control credentials or device numbers, access control credentials or devices must not be verbally identified by number in the presence of offenders.

b) Access control credentials and devices are not employed for any use other than their intended purposes and must not be altered or defaced in any way.

f) Access control credentials or devices must not be duplicated for any purpose except when authorized by the appropriate authority.

g) Access control credentials or devices must not leave the facility unless specifically authorized. In the event an employee accidentally leaves the facility with a credential or device, the employee must immediately return it upon discovery or notification.

h) Employees who identify any access control credentials or devices that are not being used must report such items to authorized staff for removal.

i) Employees must be alert for any lock that is jammed, tampered with, or in need of repair. Anyone finding such a lock must immediately report it.

j) No personal locks or handcuff/leg iron keys may be introduced into the facility without the approval of the captain or a higher authority.

k) Locksmith tools and supplies must be kept in a secure location inaccessible to all persons not directly involved in the access control process, including such examples as: blanks, tools, cutters, key cores, and file keys. These tools and supplies must be accounted for on a regular basis to ensure their security.

3. Replacing access control credentials and devices
   a) Access control credentials or devices that are lost or damaged must be immediately reported to the proper authorized authority with the required incident reports. Documentation of lost or damaged access control credentials and devices is retained at the facility according to the records retention schedule.

   b) Replacement access control credentials may be obtained through written request via a key request form. A new credential is manufactured and issued on the approval of the appropriate facility authority. Only authorized staff may add or remove credentials (keys) from a key ring, unless removal is specifically authorized.

4. Key rings
   a) Key rings or other access control credentials or devices that are of special concern must be secured to prevent tampering.

   b) Key rings are periodically checked. Area supervisors must be notified of any discrepancies.

   c) Non-security keys issued to offenders to access rooms/cells, footlockers, etc. are accounted for and a system developed to govern their issuance, repair, and return upon the offender's departure.

5. Approved and completed new or changed request forms for access control credentials or devices are retained for inventory and security purposes by the locksmith/designee or other assigned access control staff person at the facility.

6. Auditing guidelines
   a) At a minimum, once every fiscal year, the access control officer must identify and account for every facility key, ensuring assigned keys are on assigned rings. Additional random checks for accuracy are recommended.

   b) The access control officer must audit key card and other non-key access credentials for accuracy at a minimum every fiscal year, ensuring card access levels are authorized for the users. Additional random checks for accuracy are recommended.

   c) The access control officer must retain the audit documentation according to the retention schedule.

INTERNAL CONTROLS:

A. Documentation of lost or damaged access control credentials and devices is retained at the facility.

B. Approved and completed access control request forms are retained by the assigned access control staff person at the facility.

C. Documentation of audits is retained by the access control officer at each facility.

ACA STANDARDS: 4-4195, 4-4222, 1-ABC-3A-20, 1-ABC-3B-11, 4-JCF-1B-03 BP 3, and 4-JCF-2A-23

REFERENCES: Policy 105.0105, "Access Control Identification Card and Mechanical Keys – Central Office"

REPLACES: Policy 301.060, "Access Control Devices," 7/17/18.
All facility policies, memos or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: None

APPROVED BY:
Deputy Commissioner, Community Services
Deputy Commissioner, Facility Services
Assistant Commissioner, Operations Support
Assistant Commissioner, Facility Services

Security Instructions (restricted access)
301.060-3RC, "Access to Complex Office Areas"
301.060-4RC, "Emergency Evacuation of Control Bubbles"