Minnesota Department of Corrections

Policy:	**103.0131**	**Title: Controlled Access Tracking System (CATS)**
Issue Date:	**10/18/16**	
Effective Date:	**10/18/16**	

AUTHORITY: Minn. Stat. §241.01

PURPOSE: To provide for use of Controlled Access Tracking System (CATS).

APPLICABILITY: Department-wide

POLICY: Upon entering a department correctional site that utilizes the controlled access tracking system (CATS) as an access monitoring system, all individuals are registered into the CATS, photographed and provided identification in accordance with DOC Policy 103.013, "Identification Cards – Employees/Contractors/Volunteers/Interns." Identification cards must be used to scan into and out of the site through the use of CATS.

DEFINITIONS:

Active directory – the database containing cardholder information that is used by the CATS database.

Central office and facility CATS access coordinators – staff who enter cardholder data and oversee cardholder data entry into CATS.

Central office and facility CATS administrator – a designated staff member responsible to maintain the local CATS program.

Department CATS Administrator – individual charged with the responsibility of monitoring the ongoing maintenance and operation of the department CATS program and implementing modifications when necessary.

PROCEDURES:

A. Department CATS Administrator

1. The Department CATS administrators:

a) Maintain the DOC infrastructure for CATS; and

b) Coordinate with central office and facility CATS administrators as appropriate to maintain the system infrastructure.

B. Central Office and Facility CATS Administrator

When central office or facility information technology (IT) staff grant network access for a new employee or a non-DOC person, they create that account in the Active Directory and add the person to the appropriate group for CATS access.

C. Central Office and Facility CATS Access Coordinators

Central office and facility CATS access coordinators enter cardholder data and oversee cardholder data entry into CATS for non-DOC persons who have not been entered into the system as described in section B, above.

1. Access requests of this type must identify the following information:

a) Cardholder name and driver's license/state ID number;

b) Specific access areas required;

c) Date and time required;
d) Ending date of access;
e) Responsible staff; and
f) Reason for access.

2. Access to cardholder data must be password-protected and only accessible to authorized staff.

D. Central Office and Facility ID Staff

1. Provide the staff member requesting access with a copy of the Intent to Collect Private Data – Photographs/Visual Images – Employee form (attached);

2. If the staff member refuses to sign the form, notify the human resources (HR) department before proceeding; if the employee signs, forward the signed notice to the HR department to retain in the employee's file;

3. Take a cardholder's photo through CATS; and

4. Create, activate, and issue department ID cards when the cardholder is approved.

E. Central Office Front Desk and Facility Security Staff

1. Provide the person requesting access with a copy of the Intent to Collect Private Data – Photographs/Visual Images – Non-employees form (attached);

2. If the person refuses to sign the form, notify him/her that access may not be granted without consent to take a photograph. Contact the staff member responsible for the person's visit/appointment for additional assistance if needed.

3. Route the signed consent form to the staff member responsible for the person's visit/appointment.

4. Take a photo of persons who are not issued a permanent ID card;

5. Issue temporary ID cards to staff and non-DOC persons as appropriate; and

6. Grant or deny access to central office and facilities based on whether the person has a valid department ID card and other factors.

F. Central Office and Facility Staff Responsible for Lock Outs

1. Upon administrative determination that an individual is banned from entry, staff responsible for lock outs must update the respective cardholder's credential(s) to disable them in the CATS.

2. If the individual attempts entry at any department site with a disabled ID card, the CATS screen will display a red border around the ID card image.

G. Site Entry/Exit

1. As authorized individuals enter the site, they must display their department ID cards. The individual must scan the ID card in the CATS by placing it directly over the designated scanner.

a) A successful scan is indicated by an image of the ID on the monitor screen located next to the scanner. A text message appears on the screen directing the individual to move forward.

b) As cardholders successfully scan their ID cards, the ID images also display on the CATS monitor located inside the designated site control center.

c) As individuals are authenticated via the CATS, control center staff systematically grant access into and out of the site via the sallyport. The CATS enforces a limit of individuals in the sallyport at one time. Each site establishes and enforces a limit of staff in the sallyport at one time (based on sallyport size, ability of control staff to view staff items, etc.).

2. If a cardholder is locked out, the staff monitoring the control center receive an alert message on the screen, indicating the individual has been "banned" from entry.

3. If an ID card malfunctions and is not authenticated by the CATS, control center staff must seek watch commander approval to issue the individual a temporary ID card.

H. Designated staff respond to management requests to extract data from the CATS database regarding an individual's past site entry/exit.

I. Emergency Facility Rosters
In the event of an emergency, designated staff may obtain information from CATS regarding individuals currently present in the facility, in order to account for staff and others.

J. Tracking Past Entry/Exit of Individuals
The CATS maintains a 90-day log of data regarding past staff entry/exit at the facility.

K. Authorized Cardholders – Responsibilities
An authorized cardholder must:
1. Not have more than one active ID card issued to him/her;
2. Not be in possession of an unauthorized ID:
3. Not transfer or share an ID card with anyone;
4. Show an ID when requested by a staff member acting in his/her official capacity;
5. Only enter sites where authorized; and
6. Surrender any ID card(s) when requested by site security staff.

INTERNAL CONTROLS:

A. Reports regarding an individual's entry/exit are accessible through the CATS database for the retention period of the system.

B. Cardholder personal information is password protected and is only retrievable by authorized staff.

C. Signed Intent to Collect Private Data – Photographs/Visual Images forms are retained in the appropriate human resources (HR) department or department that arranged for the non-employee's visit/appointment.

REVIEW: Annually

REFERENCES: Policy 103.013, "Identification Cards - Employees/Contractors/Volunteers/Interns."

SUPERSESSION: Policy 103.0131, “Controlled Access Tracking System,” 5/17/16.
All facility policies, memos, or other communications, whether verbal, written, or transmitted by electronic means, regarding this topic.

ATTACHMENTS: Minnesota DOC Intent to Collect Private Data – Photographs/Visual Images - Employees (103.0131A)
Minnesota DOC Intent to Collect Private Data – Photographs/Visual Images – Non-Employees (103.0131B)

/s/

Deputy Commissioner, Facility Services

Deputy Commissioner, Community Services

Security Instructions
103.0131LL, “CATS Start Up Procedures”