DEPARTMENT OF CORRECTIONS

Policy Number:	**105.220**
Title:	**Statewide Supervision System (S^3) Access**
Effective Date:	**8/10/26**

PURPOSE: To provide consistent guidelines for Statewide Supervision System (S^3) access.

APPLICABILITY: Minnesota Department of Corrections (DOC); agencies requesting access to S^3.

DEFINITIONS:

Department of Corrections Portal (DOC Portal) – a secure website hosted by DOC allowing qualified criminal justice users a single sign-on, bringing together or aggregating access to content from participating county and DOC systems or servers.

Integrated Search Service (ISS) – a service operated by the Bureau of Criminal Apprehension (BCA) that allows authorized users to search and view data that are stored on one or more databases maintained by criminal justice agencies, as defined in section 299C.46, subdivision 2.

Statewide Supervision System (S^3) – A computerized data system to assist criminal justice agencies in the conduct of their official duties monitoring and enforcing the conditions of conditional release imposed on people by a sentencing court or the commissioner of corrections. S^3 includes case plan data as specified in Minn. Stat. § 241.065, Subd. 2(c).

PROCEDURES:

A. Request for Access to the Statewide Supervision System (S^3) by Agencies

1. Requests for S^3 access will be accepted only from statutorily authorized agencies as defined in Minn. Stat. §§ 241.065 and 246.13.

2. All requestors must follow the procedure listed in Policy 105.219, "Department of Corrections Portal (DOC Portal)," for S^3 access.

B. Request for Access to S^3 Data by Individuals

1. An individual seeking their own data from the S^3 must make a request using the Request for Government Data form (attached) available through the public DOC website.

2. An individual seeking their own data must present valid photo identification (including driver's license, military ID, Minnesota ID, Minnesota tribal ID, Metricula Consular, passport, or other valid state identification card) to the responsible authority or designee. Additional documentation may be required to obtain the data of a minor, including, but not limited to, a certified copy of the minor's birth certificate or certified copies of other documents establishing parent/guardian relationship, such as a court order or valid power of attorney.

3. Consent by an individual is not a sufficient reason to release data on the individual to a third party, Minn. Stat. §§ 13.84 and 13.85.

4. Data provided to the individual must be in compliance with the Minnesota Government Data Practices Act.

5. Should the identifiers provided, such as, name, date of birth, and driver's license number, attain an exact match in the system, appropriate access to the data is granted to the individual. If an exact match cannot be established, the individual is provided with a list of agencies (counties) which may have information on the individual.

C. Data Retention

1. Each submitting county or agency determines its own retention schedules in accordance with Minn. Stat. § 15.17.

2. DOC accepts data via S^3 from local operational systems.

3. Agencies must advise the DOC if there is any impact a specific retention schedule may have on S^3 data or collection procedures.

D. Auditing

1. User audit

An assigned DOC staff person conducts an S^3 user audit. The staff person verifies that each agency has a completed DOC Portal User Registration Form (attached) for the users of that agency and that each of the users are in compliance with Policy 105.219, "Departments of Corrections Portal (DOC Portal)."

2. BCA audit

Minnesota Bureau of Criminal Apprehension (BCA) staff audit users with S^3 access via the Integrated Search Service (ISS). The BCA audit includes an audit of S^3 transactions via ISS, which is a part of the agency's triennial audit for the National Crime Information Center (NCIC), Interstate Identification Index (III), and BCA system access. Any other review of ISS use is addressed in applicable BCA policies.

E. Security of S^3 information

In addition to abiding by the security of DOC portal information as outlined in Policy 105.219, "Department of Corrections Portal (DOC Portal)," agencies and individuals accessing the S^3 must adhere to the MNIT enterprise security policies.

INTERNAL CONTROLS:

A. The "DOC Portal User Registration" forms and the DOC "Portal User Registration Review/Approval" forms that are processed internally are retained by the assigned system support staff as per MNIT enterprise security policies.

B. Subject of data request forms are retained at the DOC central office.

C. S^3 data reflects the retention policies of the submitting agency.

D. S^3 audit reports are retained at the DOC central office.

STATE CORRECTIONAL FACILITY SECURITY AUDIT STANDARDS: None

REFERENCES: Minn. Stat. Chapter 13, Minnesota Government Data Practices Act
Minn. Stat. §§ 13.02, subd. 3a; 13.84; 13.85; 15.17; 241.065; 246.13, subd. 1 and 2; 246B.04, subd. 3; 611.272; and 626.84
Minnesota Rule 1205.0400
Policy 105.219, "Department of Corrections Portal (DOC Portal)"

REPLACES: Policy 105.220, "Statewide Supervision System (S^3) Access," 6/2/20.
All facility policies, memos, or other communications, whether verbal, written, or transmitted by electronic means, regarding this topic.

ATTACHMENTS: Request for Government Data (105.220A)

APPROVALS:
Commissioner of Corrections