
Policy Number: 105.219
Title: Department of Corrections Portal (DOC Portal)
Effective Date: ~~6/2/20~~6/9/26~~XXXX~~

PURPOSE: To define secure protocols regarding access to Portal functionality and/or data through the DOC Portal.

APPLICABILITY: Minnesota Department of Corrections (DOC), agencies requesting access to the DOC Portal.

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 a number of other DOC systems or servers.

DOC Portal applications – components of DOC Portal are as follows:

- ~~1.~~ ~~Case Plan – system providing access for statutorily authorizes users to offenders’ case plans.~~
- ~~12.~~ Community Sex Offender Treatment (CSOT) – system providing access for outpatient treatment programs that receive grant funding from the DOC to track incarcerated people~~person~~offenders receiving services from those treatment programs.
- ~~23.~~ Detention Information System (DIS) – system providing access for authorized users to report information on persons detained or confined within their facility.
- ~~34.~~ Electronic Worksheet System (EWS) – an application for preparing and monitoring the sentencing worksheets. A sentencing worksheet is a document ordered by the court pursuant to Minn. Stat. § 609.115, subd. 1(e) to facilitate application of the Minnesota Sentencing Guidelines as defined by the Minnesota Sentencing Guidelines Commission (MSGC).
- ~~45.~~ Inspection and Enforcement (I&E) application – the system tracks completion of facility inspections; reviews and generates final inspection reports and licenses; tracks facility-related contract information, complaints and incidents, and potential violations regarding state and federal holding of juveniles; assists facilities in calculating staffing analyses; and maintains I&E staff assignments for facilities licensed/certified by the I&E unit.
- ~~56.~~ Law Enforcement (LE) viewer – system providing access for authorized users to search for incarcerated people~~adult offenders~~persons, juvenile residents, fugitives (including security threat group fugitives), and releases (both future offender/resident releases as well as past offender/resident releases).

- 67. Offender Assessment Tool (OAT) – system providing access for authorized probation and prison facility staff to standardized risk assessment instruments for adult offenders and juvenile residents.
- 78. Statewide Supervision System (S³) – a computerized data system to assist criminal justice agencies in monitoring and enforcing the conditions of conditional release imposed on adults and juveniles by a sentencing court or the commissioner of corrections.

DOC Portal User Registration form – document to be filled out by potential users providing detailed information about their agency and the roles they are requesting.

DOC Portal User Registration Review/Approval form – document used to ~~record user ID and password for users and to~~ obtain additional signatures and/or approvals from business area process owners for DOC Portal user access.

PROCEDURES:

- A. Request for access
 - 1. All users must submit a completed DOC Portal User Registration form to obtain access to DOC Portal applications. ~~The completed DOC Portal User Registration~~ form must be submitted to the assigned system support staff. ~~Internal approvals~~ ~~may~~ ~~might~~ be required and, ~~if so,~~ can be acquired by the assigned system support staff through the DOC Portal User Registration Review/Approval form.
 - 2. The DOC Portal User Registration form can be requested by contacting the DOC IT service desk.
 - 3. ~~The completed DOC User Registration forms and DOC User Registration Review/Approval forms are~~ ~~are~~ retained by the assigned system support staff ~~as in accordance with~~ ~~per~~ Minnesota IT Services (MNIT) Enterprise Security Policy guidelines.
- B. DOC Portal system usage
 - 1. ~~The~~ DOC Portal is to be used as an access point for portal applications.
 - 2. Proper use
 - a) ~~The~~ DOC Portal is not for personal use. ~~Users must ensure that the information accessed~~ ~~n they access~~ through the system is used only for legitimate work-related purposes ~~associated with their related to~~ job duties ~~as per~~ ~~in accordance with~~ ~~according to~~ state ~~and/or~~ federal laws.
 - b) Information contained in DOC Portal may only be used or ~~disclosed~~ ~~provided~~ as permitted by state or federal laws.
 - 3. Security of DOC Portal information
Agencies and individuals accessing the DOC Portal must adhere to the following security guidelines. ~~F~~ ~~Failure to abide by the acceptable use policies contained herei~~ ~~n~~ may result in temporary or permanent loss of access privileges:

- a) Any account that has not been accessed within a 90-day period is automatically disabled. ~~Any account that has not been accessed within a 210-day period requires a new DOC Portal User Registration form to restore [the user user](#) access.~~
- b) Shared accounts are not ~~permitted~~[allowed](#). ~~If it is discovered that a shared account is being utilized, DOC staff may temporarily or permanently disable the account.~~
- c) Personal e-mail ~~addresses are~~ not accepted ~~when~~[while](#) creating a new account. Any exception to this requirement must be pre-approved by the agency management head or authority.
- d) Any logon information or data extracted from the system ~~may~~[must](#) be stored ~~only~~ on an agency-owned personal computer (PC), ~~or~~ workstation, [mobile device, or removable media](#). ~~Any data stored on a mobile device or removable media (such as a laptop, smart phone, or USB flash drive), must be encrypted and kept on an agency-owned device.~~ Each agency is responsible ~~to ensure~~[for ensuring](#) the security of information stored on ~~these~~[a](#) devices and is responsible for any unauthorized access of this information.
- e) Each agency is responsible to ensure the security of any information that is printed and is responsible for any unauthorized access to the printed information.
- f) Authorized users are responsible for [maintaining](#) the security of their passwords and accounts. ~~Passwords must be kept secure and confidential.~~
- g) The DOC Portal website has an automatic time-out feature. ~~As an additional security measure, the DOC recommends that all agency PCs, laptops, mobile devices, and workstations utilizing the system be secured with a password-protected screensaver with automatic activation set at ten minutes or less or by requiring users to lock their workstation when they are away from the workstation.~~

INTERNAL CONTROLS:

- A. DOC Portal User Registration forms and DOC Portal User Registration Review/Approval forms that are processed internally are retained by the assigned system support staff as per MNIT Enterprise Security Policy.
- B. DOC Portal user accounts are automatically disabled by the system after 90 days of non-use.

STATE CORRECTIONAL FACILITY SECURITY AUDIT STANDARDS: ~~None~~ ACA STANDARDS: ~~None~~

REFERENCES: Minn. Stat. §§ [241.01](#), [241.021](#), [241.065](#), [241.67](#); [244.09](#); [246.13](#); [609.115](#), subd. 1(e); and [626.84](#)
Minn. Rules [2900](#); [2910](#); [2911](#); [2920](#); [2945](#); [2955](#); [2960](#); [2965](#); [3000](#)

[Policy 105.220, "Statewide Supervision System \(S³\) Access"](#)

[Policy 600.200, "Certification and Inspection of Facilities and Enforcement of Rules"](#)

[Policy 600.210, "Review of Complaints, Incidents, and Deaths"](#)

REPLACES:

Policy 105.219, "Department of Corrections Portal (DOC Portal) 2/21/17.

All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS:

None

APPROVALS:

~~Commissioner of Corrections Deputy Commissioner, Community Services~~

~~Deputy Commissioner, Facility Services~~

~~Assistant Commissioner, Operations Support~~

~~Assistant Commissioner, Criminal Justice Policy, Research, and Performance~~