ADULT COMMUNITY CORRECTIONS DIVISION
STANDARD OPERATING PROCEDURES

Procedure No.: ACCD 1.7.100	Subject: **OMIS ACCESS FOR CONTRACT FACILITIES**
Reference: DOC 1.7.3; DOC 1.7.6; DOC 1.7.7; DOC 1.7.9	Page 1 of 4
Effective Date: 09/26/11	Revision Dates: 03/13/14; 07/17/14
Signature / Title: /s/ Pam Bunke, ACCD Administrator	

I. DIVISION DIRECTIVE:

Employees of contracted facilities will follow established procedures to receive access to the Department of Corrections' Offender Management Information System.

II. DEFINITIONS:

ACCD-Adult Community Corrections Division Contracted Facility – Includes Prerelease Centers (PRC), Sanction Treatment Assessment Revocation & Transition (START), Warm Springs Addiction Treatment & Change Program (WATCh), Connections Corrections Program (CCP), Passages Alcohol and Drug Treatment (Passages ADT), Passages Assessment, Sanction & Revocation Center (Passages ASRC), NEXUS Correctional Treatment Center (NEXUS), and Elkhorn Treatment Center (Elkhorn).

Computer Use – As used in §45-6-311, MCA, the term "obtain the use of" means to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network or to cause another to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network.

Department or DOC – The Montana Department of Corrections.

Information Technology Resources – Any computer system including, but not limited to, computers, servers, printers, smartphones, tablets, laptops, and networks.

Malicious Software – A dangerous computer program with the characteristic feature of being able to generate copies of itself, and thereby spread. Additionally, most malicious software has a destructive payload that activates under certain conditions.

Offender Field File – The OMIS and/or hard copy record used for offender management containing legal documents, reports, and offender records to include, but not limited to, material regarding custody, classification, treatment programs, and community supervision. Also referred to as "case record."

OMIS – Offender Management Information System – The Department of Corrections' electronic data collection and reporting system.

Password – An alphanumeric combination of characters unique to individual users that allows access to a specific computer, network or computer system.

User ID – Used generically to refer to CI number, login ID, ACF2 ID, user account, or any other term used to describe a user's unique identifier which is used to grant rights and privileges on a computer, computer system or network. User IDs are never reused.

III. PROCEDURES:

Access to OMIS by contracted facility employees is accomplished through "ePass Montana," a secure service provided by the state of Montana (mt.gov).

Employees may only use information technology (IT) resources to conduct Department business and are responsible for appropriate computer use and safe-keeping. There is no right of privacy in the use of IT resources and all aspects of employee usage may be monitored.

Any contracted facility employee authorized to enter, modify, or delete data is responsible and accountable for the completeness, accuracy and timeliness of the data they handle (see *DOC 1.7.3 Data Quality*).

Under no circumstances will an offender be allowed to use IT resources to access the on-line services of mt.gov.

A. OMIS Access through ePass Montana

1. The Administrative Officer within the ACCD will act as the security coordinator in receiving requests from contracted facilities for new or changed access to OMIS. If approved, request will be forwarded to the IT's Service Desk for implementation.

    a. An initial request will be made to the ACCD Administrative Officer to add an employee for access to OMIS.

    b. The Administrative Officer will provide *DOC 1.7.7(B) Contractor IT Policy Consent Form* and *OMIS/ePass Request*.

    c. Once the employee has completed a review of the DOC policies listed on the *Contractor IT Policy Consent Form*, the *Form* must be completed, printed and signed by the employee and supervisor. Electronic signatures will not be accepted. SCAN and email the *Form* to the IT Service Desk at corhelp@mt.gov, or fax to (406) 444-4920.

    d. The *OMIS/ePass Request* must be completed by the supervisor and include justification for the employee's OMIS access. It is then submitted by email as a WORD document to the Administrative Officer. DO NOT SUBMIT SCANNED FORM. Administrative Officer will forward to IT upon approval.

    The "User ID" is assigned by IT after *Request* is submitted. This User ID (CIV#) becomes the OMIS User ID for log-in to OMIS.

    e. When access has been implemented, the Administrative Officer will notify supervisor and provide ePass instructions upon request.

    f. Deleting or changing employee's access:

    Once an employee's need for OMIS access has changed or is no longer required, the ACCD Administrative Officer must be notified **as soon as possible**. *OMIS/ePass Request* is

completed showing "Delete" or "Change" as the "Type of request," and emailed to the Administrative Officer, who will forward it to IT.

2. User IDs and Passwords

   a. ePass Account:
      i. Employee will follow instructions for creating an ePass account, choosing Username and Password, and providing a Password Hint.
      ii. Only the Password Hint can be retrieved by mt.gov.
      iii. If Username or Password is forgotten, employee must create a new ePass account and notify corhelp@mt.gov to reconnect to OMIS.

   b. OMIS Access:
      i. The OMIS User ID (CIV#) and initial password will be provided by IT.
      ii. Employee will change OMIS password once initial log-in has been completed.
      iii. User ID or password may be retrieved from corhelp@mt.gov if forgotten.

   c. Employees must protect the confidentiality of their User ID and password, may not share this information, and may not write the information where it can be found by others.

3. Employees will not remain signed into OMIS when absent from the computer for 15 minutes or longer and will power off computer when leaving at the end of the workday. After 30 minutes of inactivity, employee will automatically be logged-off and must go through log-in procedures to return to OMIS.

4. Employees who have not accessed OMIS within a 30-day time period will be automatically locked out of OMIS and must contact corhelp@mt.gov.

5. Computer rights will be immediately terminated for employees violating DOC policies and procedures.

B. General Prohibitions of Computer Use

1. A person commits the offense of unlawful computer use if he/she knowingly or purposely:

   a. Obtains the use of any IT resource without consent of the owner;

   b. Alters or destroys or causes another to alter or destroy an IT resource without consent of the owner; or

   c. Obtains the use of, alters, or destroys an IT resource, or any part thereof as part of a deception for the purpose of obtaining money, property, information, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

2. Malicious Software Introduction

   Users will not intentionally introduce malicious software into a state IT resource.

3. Prohibited Uses

   a. Use of IT resources, IT resource data or User IDs for the purposes other than those for which they were intended or without consent of the Department's security officer;

b. Using state IT resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.

c. Downloading, installing, or running security programs or utilities, which reveal or could be used to reveal weakness in the security of the state's IT resources;

d. Attempting to modify, install, or remove state IT equipment, software, or peripherals without proper authorization; including installing any hardware, software, or non-approved external storage device on state-owned IT resources.

e. Accessing computers, computer software, computer data or information, or networks that the state has access to, without proper authorization;

f. Circumventing or attempting to circumvent normal resource limits, login procedures, and security regulations or sharing of personal usernames or passwords;

g. Taking advantage of another user's naiveté or negligence to gain access to any User ID, data, software, or file that is not your own and for which you have not received explicit authorization to access;

h. Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner;

i. Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission;

j. Any use for private or commercial profit, product advertisement or political lobbying;

k. Downloading any confidential or personally identifiable information to any removable storage media that is neither Department-owned nor encrypted;

l. Sharing, giving or selling Department-owned confidential or personally identifiable information with anyone outside of the agency without explicit permission; and

m. Other prohibited uses outlined in *DOC 1.7.6 Unlawful Use of Computers*.

4. Users will report unlawful use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated. If it is determined an employee has violated this procedure, immediate termination of network and system access may result.

IV. CLOSING:

Questions regarding this procedure shall be directed to the Facility Administrator, Prerelease Center Contract Manager, Treatment Facility Contract Manager, or ACCD Administrative Officer.

V. FORMS

DOC 1.7.7(Attachment b) Computer Security Information Technology Bureau

Contractor IT Policy Consent Form

OMIS/ePass Request