I. AUTHORITY

The Commissioner of Corrections adopts this policy pursuant to the authority contained in 34-A M.R.S.A. Section 1403.

II. APPLICABILITY

Entire Maine Department of Corrections

III. POLICY

It is the policy of the Department of Corrections to provide for the security of the information and data collection system, including verification, access to data and protection of the privacy of clients and staff. It is further the policy of the Department to strictly enforce the use of portable digital storage devices (e.g., USB thumb drives, PDAs, CDs/DVDs, external hard drives, cell phones, etc.)

This policy shall be reviewed annually and revised as necessary.

IV. CONTENTS

Procedure A: Department Security
Procedure B: CORIS Security
Procedure C: Wide Area Network (WAN) Security
Procedure D: Local Area Network (LAN) Security
Procedure E: User Security

V. ATTACHMENTS

Attachment A: CORIS Statement of Compliance
VI. PROCEDURES

Procedure A: Department Security

1. The security policy for each system within the Department of Corrections may vary with the most stringent security being the driver for any user access.

2. The security of these systems shall be monitored by the Information Technology Division through policy, practice and audits.

3. The Agency Technology Officer, or designee, shall investigate any breaches of security in the Department’s information/data collection systems.

4. Access to a computer system shall require user level security and may require computing device level security (e.g. Password protected screensavers, fingerprint ID).

5. Access to applications shall be requested by Site Coordinators through the Information Technology Help Desk.

6. Only staff authorized by Information Technology (listing maintained) shall have access beyond the application level. All programming functions and operating system access shall be restricted to Information Technology Division staff, or contract personnel specifically under the supervision of Information Technology.

7. All staff (to include contractors) authorized access to CORIS or any other Departmental client information shall be required to sign a statement of compliance (Attachment A, CORIS Statement of Compliance), which identifies understanding and acknowledgment of policy and procedures for using CORIS or any Departmental client related information.

8. Users shall be given access only to applications and data required in the performance of their job responsibilities. Applicable forms shall be submitted by the Site Coordinator to the Information Technology Security Administrator to grant, modify or terminate access.

9. Access (User IDs, passwords, etc.) shall be controlled by Information Technology, and may be revoked for user violation of this policy.

10. Client access to any computer connected to the Department’s systems is strictly prohibited.
a. Computers must be physically secured from access by a client in unsupervised areas.

b. Monitors should be arranged so that they are not visible to casual observers.

c. Visual security shall be maintained by enforcing a password-protected screen saver activated (with a hot key) upon leaving the immediate proximity of a PC.

d. A one-minute timer on screen savers shall be the default in areas where clients have access.

e. Loading software or any electronic data created by a client on a computer connected to Corrections’ Systems is strictly prohibited.

11. If, under certain circumstances, a client is permitted to view some portion of his/her case information, that information must only be presented in printed form. Under no circumstances should a client be permitted to view any CORIS screens.

12. All staff (to include contractors) are responsible to prevent unauthorized physical access to any of the Department’s data.

Procedure B: CORIS Security

1. Each employee permitted access to CORIS shall be assigned one or more job functions.

2. Depending on the employees job function, he/she shall have access to various areas of the system in either a read-only or full insert and maintain capability. The employee shall not have access to any portion of CORIS that represents areas outside of his/her assigned job functions. (See Attachment B – CORIS Job Function/Classification Security Table)

3. Individual employees can be assigned job functions that do not correlate to their own job classification.

4. When there are ten (10) days to the expiry date, the system shall notify user that the password needs to be changed.

5. All areas of CORIS that contain information deemed to be of a “critical” or “sensitive” nature shall have full auditing in place. In addition, areas such as Victim Notification, Informal Adjustments, and Probation Notes shall be accessible to specified Job Function(s) only.
6. To help ensure there is not inadvertent access to client information on laptops that store client records in the “Offline” mode, the laptops must use Windows 2000 or greater for the operating system.

7. CORIS Password Security

   a. Change password shall be available from the main menu.

   b. The user shall select the ‘change password’ menu link where the password can be changed. The user shall enter the old password and two (2) instances of the new password. A password must contain both alpha and numeric text. The user shall also enter mother’s maiden name on password screen. During migration, this field shall default to ‘MOTHER’S MAIDEN NAME’. The user shall be forced to change this on the first time in.

   c. All CORIS passwords shall expire after ninety (90) days. If the password has expired, the user will get the following message: ‘Your password has expired. Please contact the help desk at (202) 287-1964 to re-initiate.

   d. User shall call help desk. IT administrator shall enter user’s staff screen and view the date the password was last changed. If the password has not reached the expiry date, the IT administrator shall know the password does not need to be changed and either another person is trying to get into the system using someone else’s user ID or the user has forgotten his/her password. The reset button shall be on the staff screen and shall allow the user to enter the system using a designated password as established by the Department. This password shall expire after the first use. The IT administrator shall then ask the user to enter the system with user name and password. Upon entering the system, the user shall change password.

   e. Days remaining on the change password screen shall be displayed.

   f. Initial complex password shall be used. This password shall expire either after the first use or in ninety (90) days, whichever is first.

   g. The password of ‘password’ shall never be allowed in the system.

   h. There will be three (3) login attempts before the user must start the entire process again.

   i. The Password characteristics are:

       • Minimum Password Length shall be 8 Characters.
Maximum Password is 14 Characters.

Password must be alphanumeric.

j. Users should choose passwords that are easy to remember and difficult for others to guess. Some passwords that are easy for others to guess are pet names, sports teams and names of family members. You can make a password more difficult to guess by using a combination of letters, numbers and punctuation or by using both upper and lower case letters.

Procedure C: Wide Area Network (WAN) Security

1. Servers shall be physically and electronically secured from unauthorized access.

2. Access to the WAN shall only allow direct access to applications that are available to the general public and/or all State of Maine employees.
   a. Site Coordinators must request access for their users from the Systems Security Administrator of the application(s) being accessed.
   b. Applications not intended for all State employees shall be UserID and password protected.

3. Physical security for all computing devices in areas not accessible to clients shall be maintained by:
   a. Depending on device, enforcing a password-protected screen saver activated (with a hot key) upon leaving the immediate proximity of a computing device.
   b. A five (5) minute timer on password-protected screen savers shall be the maximum permitted (must be a one (1) minute timer in areas where clients may have access.)
   c. Users must be logged off the network during non-working hours.

Procedure D: Local Area Network (LAN) Security

1. All security provisions relating to the Wide Area Network also apply to Local Area Networks.

2. System Administrators, in conjunction with the users, shall provide for the security of workstations.
3. Access to applications and data available on the LAN shall be restricted by identity of the user. A userID and password shall identify the user on the LAN server.

4. System Administrators shall issue user IDs and passwords. A library of users, access levels, user IDs and passwords shall be maintained by the System Administrators.

5. System Administrators shall load software onto the servers. Users are not allowed to load software onto the server.

**Procedure E: User Security**

1. Only staff with written authority (see Attachment C) from the Chief Administrative Officer, Regional Correctional Administrator or Central Office supervisor may copy Departmental data to a portable digital device and all portable digital devices must be state-issued. No Departmental data shall be copied onto a personally-owned portable digital device. In all cases, the user is accountable for security of the data.

2. All signed authorization forms shall be maintained in the employee's personnel file.

3. The authorized employee shall understand that they are responsible for safeguarding all Departmental classified information that they have copied in electronic, printed or written form.

4. The user, in conjunction with the System Administrator, shall ensure that only authorized persons can use any Departmental computing device.

5. Computing devices shall contain only software approved by Information Technology. Non-approved software may not be brought from home or elsewhere (downloading off the Internet) and loaded on the system.

6. The security of passwords is the users' responsibility (See Attachment A, CORIS Statement of Compliance).

   a. Passwords shall not be shared with other persons, except in the event of an emergency.

   b. Users shall change such passwords as soon as the emergency is over.

   c. Users must change any password known to another.
d. A password-protected screen saver shall be activated (with a hot key) upon leaving the immediate proximity of a computing device.

e. A one (1) minute timer on password-protected screen savers shall be enforced.

7. Users must be logged off the network during non-working hours.

8. Users in areas that may have client access shall keep the computer area secured when not at the computing device.

9. Common logons are prohibited. Each user must have an individual user ID.

VII. PROFESSIONAL STANDARDS

ACA:

ACI - 4-4101 All staff who have direct access to information in the information system are trained in and responsive to the system’s security requirements.

4-ACRS-7D-05 Procedures govern access to and use of an organized system of information, analysis, collection, storage, retrieval, reporting, and review.

4-JCF-6F-01 Juvenile case-record management includes, at a minimum, the following:

1. Establishment, use, and content of case records
2. Signed and dated entries in the case record
3. Maintenance, secure placement, and preservation of records to minimize the possibility of theft, loss, or unauthorized destruction of records
4. Scheduled for retiring or destroying inactive records
5. Safeguards from unauthorized and improper disclosure
6. Security, which ensures confidentiality for any part of the information system that is computerized
7. A “release of information consent form” that complies with applicable federal and state regulations, a copy of which is maintained in the case record.

4-JCF-6F-07 The facility or parent agency collaborates with juvenile justice and service agencies in information gathering, exchange, and standardization.