POLICY TITLE: INFORMATION TECHNOLOGY SECURITY **POLICY NUMBER: 5.3** **CHAPTER 5: MANAGEMENT INFORMATION SYSTEMS**		**PAGE 1 OF 5**
	STATE of MAINE **DEPARTMENT OF CORRECTIONS** **Approved by Commissioner:**	**PROFESSIONAL STANDARDS:** **See Section VII**
EFFECTIVE DATE: **November 15, 2003**	**LATEST REVISION:** **October 28, 2019**	**CHECK ONLY IF APA [ ]**

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 information technology (IT) security to ensure the appropriate use and protection of the Department's information technology and information technology assets and to specify the requirements for protecting those information assets, as well as the associated data and content.

IV. DEFINITIONS

1. Access Control - the process that limits and controls access to resources of a computer system

2. Access Privileges – system and/or application permissions associated with an account.

3. Administrator Account - a user account with additional security access, applications, and business processes compared to those with the basic user role that is necessary for the administration and/or management of a system or application For example, an administrator can create new users, change account permissions, run reports, do approvals, etc.

4. Principle of Least Privilege - A security principle where users are assigned the minimal access necessary to perform their job responsibilities.

5. Strong password - a password that resists easy access by trial and guesswork. Characteristics of a strong password: at least 8 characters; a mixture of both uppercase and lowercase letters; a mixture of letters and numbers; inclusion of at least one special character, e.g., ! @ # ?].

6. System or Application Accounts - user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications

V. CONTENTS

Procedure A:	Information Technology Security
Procedure B:	Access to Department Information Technology Resources
Procedure C:	User Access Management
Procedure D:	Confidential Information & Security of Data

VI. ATTACHMENTS

Attachment A: Authorization to Copy Departmental Classified Information

VII. PROCEDURES

Procedure A: Information Technology Security

1. The Department of Financial Services (DAFS) Office of Information Technology (OIT) serves as the agency responsible for oversight for the IT environment of state government agencies. OIT provides for, but is not limited to the following:

   a. IT architecture;

   b. standardized operating systems;

   c. user accessibility;

   d. Environment Wide Area Network (WAN) Security;

   e. Local Area Network (LAN) Security;

   f. networking;

   g. data classification of sensitive or confidential information;

   h. storage;

   i. compliance with OIT IT policies;

   j. maintenance of state technology supporting state computers;

   k. backup and recovery;

   l. disaster planning that addresses: *[5-1F-4100-2]*

      1) incident reporting procedures;

2) staff roles and responsibilities for incident response and management;

3) incident investigation procedures;

4) incident remediation and closure procedures; and

5) post-incident review and action planning procedures that focus on preventing future reoccurrences.

2. The Department's Manager of Correctional Information Technology (IT) Operations, or designee, is responsible for, but not limited to the following:

   a. ensure that the Department complies with the DAFS OIT policies and standards;

   b. serve as a liaison with the DAFS OIT Chief Information Security Officer;

   c. involvement in the decisions of the Department's acquisition of Information Technology assets;

   d. ensure that adequate and appropriate levels of protection for the Department's technical resources are in place to prevent unauthorized or unnecessary access or disclosure, and ensure effective and accurate processing and continuity of operations as relates to information technology security within the Department;

   e. ensure that the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data within the Department's information technology systems are compliant with all applicable State and Federal regulations and applicable Departmental policies; ***[5-1F-4100-1 and 4-ACRS-7D-05]*** and

   f. review this policy on an annual basis and revise it as necessary.

3. Computing devices shall contain only software approved by the Department's Manager of Correctional Information Technology (IT) Operations, or designee. Non-approved software may not be brought from home or elsewhere (downloading off the Internet) and loaded on the system.

Procedure B: Access to Department Information Technology Resources ***[5-1F-4100-5]***

1. The Department's Manager of Correctional Information Technology (IT) Operations, or designee, is responsible for managing access control to the Department's institution technology and IT assets and ensure that all stages in the life-cycle of user access, from the initial registration of new users, use, and termination of user accounts are followed. ***[5-1F-4100-5]***

2. Access privileges to Department institution technology (including networks, systems, applications, computers, and mobile devices) are provided to users based upon the following: ***[4-4101 and 5-1F-4101]***

a. need to know – a user will be granted access to the system(s) that are necessary to fulfill his or her job responsibilities and duties;

b. the principle of least privilege; and

c. trained in and responsive to the system's security requirements. *[4-4101]*

3. Physical protection and guidelines for working in secure areas shall be designed and applied, such as security barriers and entry controls. IT assets shall be protected from unauthorized access, damage, and interference.

4. Monitors shall be arranged so that they are not visible to casual observers.

5. Client access to any computer shall only be in accordance with Department Policies (AF) 24.10, Prisoner Use of Computers and/or Access to the Internet, (AF) 24.10.1, Computer Tablets, and this policy. Any other use is strictly prohibited.

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

Procedure C: User Access Management

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

2. Users shall be required to follow secure practices in the selection and use of passwords to protect against unauthorized discovery or usage by using strong passwords. Also, passwords shall:

   a. not be shared or disclosed to anyone, including friends or family;

   b. not be written down or stored electronically without encryption; and

   c. be changed immediately if found to be compromised.

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

4. Only staff with written authority (Authorization to Copy Departmental Classified Information, Attachment A) from the facility Chief Administrative Officer, or designee, Regional Correctional Administrator, or designee, or Central Office supervisor, as applicable, 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 the security of the data.

5. All signed authorization forms shall be maintained in the employee’s personnel file.

Procedure D: Confidential Information & Security of Data *[5-1F-4100-1]*

1. Department staff, volunteers, and student interns shall be responsible, but not limited to the following:
   a. safeguarding Departmental confidential information that they have in electronic or paper copies;
   b. assurance that any individual with whom Department data is shared is authorized to receive the information; and
   c. shall not use or disclose Department data that is otherwise confidential or restricted, without appropriate authorization.

VII. PROFESSIONAL STANDARDS

ACA:

5-1F-4100-1 **Written data security policy, procedure, and practice govern the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data contained in paper, physical, or media format.**

5-1F-4100-2 **There is a written information technology incident response and management plan to be used in the event that the institution experiences an information technology security breach. The plan is approved by the agency Chief Information Officer or equivalent, reviewed annually and updated as necessary, and is communicated to all staff. The plan includes the following:**

- **Incident Reporting Procedures**
- **Staff Roles & Responsibilities for Incident Response and Management**
- **Incident Investigation Procedures**
- **Incident Remediation and Closure Procedures**
- **Post-Incident Review and Action Planning Procedures that Focus on Preventing Future Reoccurrences**

5-1F-4100-5 **In cases of automated systems, written data security policy, procedure, practice govern the issuance, use, and termination of user accounts, the issuance and use of computing devices that connect to the automated information systems, the use of standalone and online applications within the information systems, and the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data that resides in the information system.**

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.**

5-1F-4101 **All staff who have direct access to the information in the information system have authorized access associated with their job duties and 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.**