POLICY TITLE: AUDITING HARDWARE AND SOFTWARE **POLICY NUMBER: 5.3.1** **CHAPTER 5: MANAGEMENT INFORMATION SYSTEMS**		**PAGE 1 OF 3**
	STATE OF MAINE **DEPARTMENT OF CORRECTIONS** **Approved by:** Martin Magnusson **Signature of Commissioner**	**PROFESSIONAL STANDARDS:** **See Section VII**
EFFECTIVE DATE: **November 17, 2003**	**LATEST REVISION:** **October 2, 2008**	**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 that all software supported by the Information Technology Division shall be audited periodically to ensure operating compliance, meeting user and management needs, procedures are being followed, properly licensed, conforms to agency standards and related documentation is current.

IV. CONTENTS

Procedure A:	Guidelines for Audits
Procedure B:	Internal Audits
Procedure C:	External Audits

V. ATTACHMENTS

None

VI. PROCEDURES

Procedure A: Guidelines for Audits

Audits of computerized applications supported by Information Technology shall ensure that:

1. The application is functioning correctly as designed.

2. The application is adequately meeting user and management needs.

3. All source code, programs, and documentation are current.

4. All necessary procedures relating to security, backups, contingency plans, and cross-training are being followed.

5. The computer equipment has sufficient capacity for continued normal operations.

6. The application is being used correctly, and all necessary operational procedures are being followed.

7. Licensed software shall be validated to make sure illegal software is not in use.

8. Software conforms to state and agency standards.

9. Any unauthorized software shall be removed.

Procedure B: Internal Audits

Information Technology Division application audits shall ensure that:

1. All libraries, directories, source code, and documentation are current.

2. The Help Desk is maintaining a problem log for each application.

3. A specific individual is responsible for program support and upgrades for each application.

4. Cross-training of user staff is being done.

5. Security measures are being taken to protect source libraries, directories and data.

6. Backup/recovery measures are taken to protect source library, directories, application code and data.

Procedure C: External Audits

Field application audits shall ensure that:

1. A problem log is being maintained.

2. Backups/recovery routines are being followed by determining the frequency and storage of backups.

3. Adequate disaster/contingency plans have been developed.

4. Verify cross-training has occurred. Ensure coverage in the event of leave, employee turnover, etc., and to avoid dependence on key personnel.

5. Security is maintained in the following areas:

   a. Physical access

   b. Computer passwords

   c. Data Security

   d. Storage of sensitive data and backup files

   e. Internet access and use

6. Field staff are using the system correctly and in accordance with published instructions, user documentation, and Policy 5.3, Attachment A – Computer Access Statement of Compliance.

VII. PROFESSIONAL STANDARDS

None