MICHIGAN DEPARTMENT OF CORRECTIONS **POLICY DIRECTIVE**	EFFECTIVE DATE 08/27/2001	NUMBER 01.04.105
SUBJECT USE OF DEPARTMENT COMPUTER EQUIPMENT, SOFTWARE AND SERVICES	SUPERSEDES 01.04.103 (01/13/97); 01.04.105 (12/13/93)	
	AUTHORITY MCL 752.791-752.797; 791.203	
	ACA STANDARDS 2-3094; 3-4097-4099; 3-4103; 1-ABC-1F-04; 2-CO-1F-06; 3-ACRS-1F-04	
	PAGE 1 OF 5	

POLICY STATEMENT:

The acquisition of Department computer equipment, software and services, and use of and access to Department computers, computerized information and data processing resources, shall be controlled to protect against errors, theft, loss and misuse, as set forth in this policy.

RELATED POLICY:

01.04.104 Internet Access

POLICY:

DEFINITIONS

A. Computerized Information: Data obtained from or created using a computer, communication device or any other related media including, but not limited to, that which is stored on data storage media (e.g., diskette, compact disk, tape) or accessed through an on-line system.

B. Data Processing Resources: Manuals for on-line system applications; data storage media, usercodes, passwords, communication devices, and any other related electronic media. It does not include personal disks and operating accessories authorized for personal word processors and typewriters pursuant to PD 04.07.112 "Prisoner Personal Property".

C. On-line System: Any mainframe (e.g., CMIS, LEIN, TADS) or client/file server application (e.g., OMNI, Visitor Tracking) which can be accessed using a computer.

GENERAL INFORMATION

D. For purposes of this policy, "Deputy Director" includes the Executive Assistant to the Director and the Administrator of the Office of Audit, Internal Affairs and Litigation.

E. For purposes of this policy, "Warden" includes the Administrator of the Special Alternative Incarceration Program facility.

F. Requests for Department computerized information shall be processed in accordance with PD 01.06.110 "Freedom of Information Act - Access to Department Public Records".

G. Requests to conduct research using Department computerized information shall be considered in accordance with PD 01.04.120 "Research Involving Corrections Facilities or Offenders".

H. Employees violating this policy may be subject to discipline as set forth in PD 02.03.100 "Employee Discipline" and/or denied use of a Department computer or access to an on-line system. An employee who is no longer able to perform his/her job responsibilities as a result of being denied use or access may be terminated from employment or reassigned in accordance with Department of Civil Service Rules and applicable collective bargaining unit agreements.

I. In consultation with the Deputy Directors or designees, the Administrator of the Office of Planning, Research and Management Information Services (OPRMIS), Administration and Programs (A&P), or designee shall determine the propriety of, and priority for, providing requested computer services.

J. Computer equipment (e.g., monitors, keyboards, printers, scanners) not approved for offender use pursuant to this policy are critical tools and shall be accounted for and secured as set forth in PD 04.04.120 "Tool Control".

INFORMATION TECHNOLOGY STANDARDS MANUAL

K. The OPRMIS Administrator or designee shall maintain the Information Technology Standards Manual. The Manual shall include standards to be followed by staff involved in providing services and support to employees for Department computers including, but not limited to, the following:

1. Standards identifying the approval process for the acquisition of computer equipment, software, and services.

2. Standards identifying computer equipment, software and services currently approved for purchase.

3. Standards for the installation, configuration, inventory and use of computer equipment and software. The standards shall include the approval process for the installation of computer equipment and software. The installation of networked computers for offender use, other than on a school assignment, shall require approval of the Deputy Director.

4. Standards identifying the approval process for the development, deployment and maintenance of computer software applications (e.g., computerized prisoner movement system).

L. The Manual shall be provided to each Deputy Director, Correctional Facility Administration (CFA) Regional Prison Administrator (RPA), Field Operations Administration (FOA) Regional Administrator and Warden for distribution to staff involved in providing services and support for Department computers. Questions regarding the standards shall be referred to the OPRMIS Administrator or designee.

COMPUTER SECURITY OFFICER

M. The OPRMIS Administrator shall appoint a Computer Security Officer. The Computer Security Officer shall be responsible for the following:

1. Subject to the approval of the OPRMIS Administrator, identifying necessary computer security measures to be taken for Department computers, on-line systems, data processing resources and computerized information.

2. Monitoring Department computer security measures, including whether employee user codes and passwords are issued and removed appropriately.

3. Investigating identified security violations and, subject to the approval of the OPRMIS Administrator, identifying appropriate action to be taken to prevent continued violations.

4. Conducting audits of computer use to ensure compliance with this policy.

5. Providing computer security technical support, as needed.

DATA PROCESSING COORDINATOR

N. Each Deputy Director shall ensure Data Processing Coordinators are designated for each area under his/her supervision, as needed. The Data Processing Coordinator shall serve as the liaison between his/her designated area and OPRMIS on all matters relating to computer equipment, software, computerized information, services and security. Deputy Directors shall ensure that the names of those designated as Data Processing Coordinators in their respective areas are provided to the OPRMIS Administrator.

O. Each Data Processing Coordinator shall monitor Department computer security measures within his/her designated area. Identified security concerns or violations shall be reported to users and supervisors, as appropriate, and to the Computer Security Officer.

P. Management Information Services (MIS), OPRMIS, in conjunction with the appropriate Data Processing Coordinator, shall provide authorized employees with specific usercodes and passwords for the computers and on-line systems they are authorized to use and access. The appropriate Data Processing Coordinator shall be notified when an employee no longer is authorized access (e.g., employee transfers). The Data Processing Coordinator shall notify MIS of the need to remove an employee's access to an on-line system and, for employees in Central Office, to remove an employee's access to a Department computer when the employee no longer is authorized access. The Data Processing Coordinator or MIS, as appropriate, shall ensure the employee's user codes and passwords are removed within three business days after the employee no longer is authorized access.

Q. Data Processing Coordinators shall ensure employees in their respective areas who are authorized to use a Department computer or access an on-line system receive a copy of this policy directive and agree in writing to the conditions set forth in the Security Agreement - Data Processing (CAJ-532) prior to using the computer or accessing the on-line system. Refusal to sign the Security Agreement - Data Processing form shall result in the employee being denied use of a Department computer and/or access to the on-line system.

USE OF COMPUTERS AND ACCESS TO ON-LINE SYSTEMS

Employees

R. Each employee authorized to use a computer or access an on-line system shall be responsible for the maintenance and security of his/her usercode and password. This shall include changing the password whenever it is suspected that the confidentiality of the password has been compromised. Employees shall not divulge their usercodes or passwords to any other individual. However, the OPRMIS Administrator shall ensure that supervisors have a means by which to access computerized information in their employees' computers as necessary to provide for continuity of services in an employee's absence.

S. Employees shall report to their immediate supervisor and the appropriate Data Processing Coordinator any suspected or confirmed violation of the computer security requirements set forth in this policy.

T. Each employee shall ensure all data processing resources and computer manuals s/he has been provided are stored when not in use in a manner which guards against theft or unauthorized access. For employees working in areas where prisoners may potentially gain access and all Data Processing Coordinators, this shall include storage in a secure location (e.g., a locked desk or cabinet).

U. Computers, data processing resources and computer manuals are not to be removed from the facility or Bureau/Office without prior written authorization from the appropriate Deputy Director or designee. Such items shall not be taken from one work location to another work location when an employee is transferred, unless approved by the appropriate supervisor and the OPRMIS Administrator or designee.

V. Employees shall not disclose to unauthorized parties computerized information that is confidential or which would pose a custody or security concern if disclosed.

W. Employees shall comply with software copyright laws. Only software approved in accordance with the Information Technology Standards Manual shall be used on Department computers. Employees shall not publish or add, transmit or download software, including screen savers and games, to Department computers without the authorization of the OPRMIS Administrator or designee. Employees also shall not open executable files (e.g., ending in ".exe", ".vbs", ".ppt") forwarded via electronic mail ("e-mail") which do not appear to be work-related.

X. Employees shall use only Department computers and access only on-line systems for which they have been approved and only to perform their assigned job responsibilities. Personal use is prohibited (e.g., personal email, chain letters, political activities). Personal computer equipment, including personal digital assistants (e.g., Palm Pilot), shall not be used with Department computers unless approved by the appropriate Deputy Director or designee.

Y. Employees using a Department computer or accessing an on-line system shall be responsible for the integrity of the information they update or enter and shall not intentionally enter false information or abuse the information obtained from the computer or on-line system. Employees shall not knowingly attempt or cause unauthorized use of a Department computer or access to an on-line system. Questions as to whether specific use or access is approved shall be directed to the OPRMIS Administrator or designee.

Offenders in CFA and FOA Correctional Facilities

Z. Offenders shall not use or personally possess computers or data processing resources in a correctional facility except as specifically authorized by this policy. Under no circumstances shall offenders use a Department computer for personal use.

AA. Offenders shall not use or personally possess in a correctional facility computer manuals, magazines or other publications which pose a threat to the security, good order or discipline of the facility. If received in the mail for a prisoner, such publications shall be rejected in accordance with PD 05.03.118 "Prisoner Mail".

BB. Offenders in corrections centers may use non-Department computers and data processing resources at school and at their place of employment, as required.

CC. Offenders in a correctional facility may use Department computers and data processing resources designated for use as part of their school assignment. Such use shall be permitted in the classroom setting only and only as necessary for the assignment.

DD. Offenders in a correctional facility may use Department computers and data processing resources as required for their work assignments (e.g., legal writer program, clerk or tutor assignment, Michigan State Industries) only with prior approval of the appropriate Warden or FOA Regional Administrator. Staff requesting such approval must submit a completed Offender Computer Use Registration Form (CAJ-328) and Offender Computer Background Investigation form (CSJ-270) to the Warden or FOA Regional Administrator for approval. The Warden or FOA Regional Administrator shall ensure a current list of approved requests is maintained. Offenders approved to use computers and/or data processing resources may do so only while on the identified work assignment and only as necessary for that assignment.

EE. Approval shall not be granted pursuant to Paragraph DD for the following:

1. To use computers which have access to the Internet.

2. To use computers or data processing resources on assignments where prisoner use is prohibited, as determined by the Computer Security Officer in consultation with the appropriate Deputy Director.

3. To use computers with hardware or software which offenders are prohibited from using, as determined by the Computer Security Officer in consultation with the appropriate Deputy Director.

4. To use networked computers which have not been installed in accordance with the Information Technology Standards Manual.

5. If use would pose a threat to the custody or security of the facility, as determined by the Warden or FOA Regional Administrator.

FF. Offenders allowed to use computers and data processing resources pursuant to this policy shall do so only while under direct and continuous staff supervision. Supervision also may be provided by non-Department employees with prior approval of the appropriate Warden or FOA Regional Administrator, in consultation with the Computer Security Officer. Those providing required supervision shall be familiar with the computer and software being used by the offender.

GG. If an offender violates this policy, his/her approval to use a computer or data processing resources may be revoked by the appropriate Warden or FOA Regional Administrator. The Computer Security Officer shall be notified of the violation. Subsequent requests for the prisoner to use a computer or data processing resources shall require approval both by the appropriate Warden or FOA Regional Administrator and the Computer Security Officer.

OPERATING PROCEDURES

HH. Each Regional Prison Administrator and the A&P and FOA Deputy Directors shall ensure that procedures necessary to implement this policy directive are developed within 60 calendar days after its effective date.

AUDIT ELEMENTS

II. A Primary Audit Elements List has been developed and will be provided to Wardens, FOA Regional Administrators and the OPRMIS Administrator to assist with self audit of this policy pursuant to PD 01.05.100 "Self Audit of Policies and Procedures".

BM:OPH:08/06/01