MICHIGAN DEPARTMENT OF CORRECTIONS **POLICY DIRECTIVE**	EFFECTIVE DATE 08/23/2021	NUMBER 01.04.105
SUBJECT USE OF DEPARTMENT COMPUTER EQUIPMENT, SOFTWARE, AND SERVICES	SUPERSEDES 01.04.105 (08/27/2001)	
	AUTHORITY MCL 752.791-752.797; 791.203; ED 2019-5	
	PAGE 1 OF 5	

POLICY STATEMENT:

The Michigan Department of Corrections (MDOC) in conjunction with the Department of Technology, Management and Budget (DTMB) monitors and maintains all devices capable of accessing the State of Michigan network or services, including software services, network access and computers, which include tablets and cell phones~~)~~. All computerized information and Information Technology resource information created or developed shall be controlled to protect against errors, theft, loss, and misuse as set forth in this policy.

RELATED POLICY:

01.04.104 Internet Access
State of Michigan Technical Standard 1340.00.130.02 Acceptable Use of Information Technology

POLICY:

DEFINITIONS

A. Computer: Any electronic, smart device, or system that contains an operating system and has the ability to enter data and/or connect to a network.

B. 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 any data storage media or accessed through an information system.

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

D. Information System: Any information system, software or services provided over the State of Michigan Network or internet.

GENERAL INFORMATION

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

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

G. Employees violating this policy may be denied access to the State of Michigan Network. An employee who is no longer able to perform their 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 regulations and applicable collective bargaining unit agreements.

H. Employees shall return any MDOC computer, including tablets and cellphones, issued to them immediately upon separation from employment with the MDOC.

I. The Deputy Directors, the Administrator of the Office of Research and Planning (ORP), Budget and Operations Administration (BOA), or designees 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 controlled items as defined in PD 04.04.120 “Tool Control” and shall be accounted for and controlled as set forth in PD 04.04.120.

K. Only a staff member’s legal name maybe entered into an MDOC database.

L. This policy shall be reviewed annually by all staff.

INFORMATION SECURITY OFFICER

M. The ORP Administrator shall select an Information Security Officer. The Information Security Officer shall be responsible for the following:

1. Subject to the approval of the ORP Administrator, identifying necessary computer security measures to be taken for MDOC computers, to protect on-line systems, information technology resources and computerized information.

2. Monitoring MDOC computer security measures, including whether employee user codes and passwords are issued in accordance with job roles and duties, using the authorized requestors process and removed appropriately through the use of monthly automated reports.

3. Conducting monthly audits of computer use and remote access to ensure compliance with this policy.

4. Referring identified security violations to the Internal Affairs Section for investigation via the Request for Investigation form (CAR-896).

5. Providing computer security technical support, as needed.

INFORMATION TECHNOLOGY LIAISON AND AUTHORIZED REQUESTOR

N. The Director and each Deputy Director shall ensure that IT Liaisons are designated for areas under their supervision, as needed. The IT Liaison shall serve as the liaison between their designated area and the IT Analyst within the Procurement, Monitoring and Compliance Division (PMCD) on all matters related to IT asset management. The Director and Deputy Directors shall ensure that the names of those designated as IT Liaisons in their respective areas are provided to the IT Analyst.

O. An Authorized Requestor is an employee authorized to review prospective users access requests, ensuring there is a legitimate business need for the request, and to approve modifications to existing application access and removes access that is no longer required.

P. The Data Security and Privacy section, in conjunction with the appropriate Authorized Requestor, shall provide authorized employees with specific user codes and passwords for the appropriate devices and information systems they are authorized to use and access. The appropriate Authorized Requestor shall be notified when an employee no longer is authorized access (e.g., employee transfers). The Authorized Requestor shall notify the Data Security and Privacy Section of the need to remove an employee's access to an information system and, for employees in Central Office, to remove an employee's access to an MDOC computer when the employee is no longer authorized access. The Authorized Requestor or the Data Security and Privacy Section, as appropriate, shall ensure the employee's user codes and passwords are disabled or deleted within three business days after the employee is no longer authorized access.

Q. Authorized Requestors shall ensure new employees in their respective areas who are authorized to use an MDOC computer or access an information 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) before using the computer or accessing the information system. Refusal to sign the Security Agreement - Data Processing form shall result in the employee being denied use of an MDOC computer and/or access to

the Information system.

USE OF COMPUTERS AND ACCESS TO INFORMATION SYSTEMS

Employees

R. Each employee authorized to use a computer or access an information system shall be responsible for the maintenance and security of their user code 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 user codes or passwords to any other individual.

S. In the event access is needed, Supervisors may fill out a Request to Monitor Usage of Information Technology Resources (DIT-0130) to access the computers of an absent employee when necessary.

T. Employees shall report to their immediate supervisor and the Data Security and Privacy Section any suspected or confirmed violation of the computer security requirements set forth in this policy.

U. Each employee shall ensure all information technology resources and computer manuals they have been provided are stored when not in use in a manner that guards against theft or unauthorized access. For employees working in areas where prisoners may potentially gain access, this shall include storage in a secure location (e.g., a locked desk or cabinet).

V. Desktop computers and computer manuals are not to be removed from the facility or worksite 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 ORP.

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

X. Employees shall comply with software copyright laws. Only software approved in accordance with DTMB shall be used on MDOC computers. Users shall not download or install any software (including shareware and freeware) unless authorized by DTMB. No State of Michigan-owned or licensed software may be installed, copied, or used on non-State of Michigan equipment unless expressly approved by DTMB. Employees also shall not open executable files (e.g., ending in ".exe," ".vbs," ".ppt") forwarded via electronic mail ("e-mail") that do not appear to be work-related.

Y. IT resources, including devices, networks, data, software, email, and system accounts, are provided to conduct official State of Michigan business. Employees shall use only MDOC computers and access only information systems for which they have been approved and only to perform their assigned job responsibilities. Employees shall not have or use non-approved software, applications, music, games or personal email accounts on state-owned devices. Authorized access to services (e.g., internet, YouTube, Skype, or Pod Cast) shall be only for the authorized business reason intended and shall not interfere with the employee's duties or the safety and security of the facility. Incidental personal use of IT resources during lunch or break times is permitted but shall not interfere or conflict with a user's work obligations or State of Michigan business and must comply with all applicable State of Michigan policies. Personal computer equipment, tablets, or phones shall not be used or connected to MDOC computers unless approved by DTMB.

Z. Employees using an MDOC computer or accessing an information 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 information system. Employees shall not knowingly attempt or cause the unauthorized use of an MDOC computer or access to an information system. Questions as to whether the specific use or access is approved shall be directed to ORP.

AA. An employee shall not use a private e-mail account to conduct state business, nor shall they use a state e-mail account for personal use. State e-mails shall only be disposed of in accordance with the Department's record retention schedule. Violations of state e-mail use shall be reported to the Governor's Chief Compliance Officer.

Offenders in Correctional Facilities

BB. Offenders shall not use or personally possess computers, including tablets, or information technology resources in a correctional facility except as specifically authorized by policy. Under no circumstances shall offenders use an MDOC computer, including a tablet, for personal use.

CC. In a correctional facility, offenders shall not use or personally possess computer manuals, magazines or other publications that 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."

DD. Offenders in a correctional facility may use MDOC computers, including tablets, computer equipment, and information technology resources designated for use as part of their school or vocational assignment. Such use shall be permitted only as approved by the Warden. The Warden shall ensure a current list of approved requests is maintained.

EE. Offenders in a correctional facility may only use specific MDOC computers, tablets, or other computer equipment, that has been specifically programmed for their access and restricted pursuant to MDOC and DTMB standards including information technology 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. Requests for such approval must be submitted on a completed Offender Computer Use Registration form (CAJ-328) and Offender Computer Investigation form (CSJ-270) to the Warden for approval. The Warden shall ensure a current list of approved requests is maintained. Offenders approved to use MDOC computer equipment and/or information technology resources may do so only while on the identified work assignment and only as necessary for that assignment.

FF. Approval shall not be granted pursuant to Paragraphs DD and EE for the following:

1. To use computers that have access to the internet except as set forth in PD 01.04.104 “Internet Access.”.

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

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

4. If use poses a threat to the custody or security of the facility, as determined by the Correctional Facilities Administration (CFA) Assistant Deputy Director (ADD) of Operations.

GG. Offenders allowed to use MDOC computers, tablets, equipment, and/or information technology resources pursuant to this policy shall do so only while under staff supervision. Supervision may be provided by non-MDOC employees with the prior approval of the appropriate Warden, in consultation with the Information Security Officer. Those providing required supervision shall be familiar with the computer and software being used by the offender.

HH. If an offender violates this policy, their approval to use MDOC computers, tablets, equipment, or information technology resources may be revoked by the appropriate Warden. The Information Security Officer shall be notified of the violation. Subsequent requests for the prisoner to use a computer, tablet, equipment, or information technology resources shall require approval both by the appropriate Warden and the information Security Officer.

OPERATING PROCEDURES

II. If necessary, to implement requirements set forth in this policy, Wardens shall ensure that procedures are developed/updated.

AUDIT ELEMENTS

JJ. A Primary Audit Elements List has been developed and is available on the Department's Document Access System (DAS) to assist with self-audit of this policy pursuant to PD 01.05.100 "Self-Audits and Performance Audits."

APPROVED: HEW 08/08/2021