

MICHIGAN DEPARTMENT OF CORRECTIONS <b>POLICY DIRECTIVE</b>	EFFECTIVE DATE 08/23/2021	NUMBER 01.04.104
	SUBJECT INTERNET ACCESS	
SUPERSEDES 01.04.104 (12/01/2011)		AUTHORITY MCL 791.203; Annual Appropriations Act
PAGE 1 OF 2		

**POLICY STATEMENT:**

Internet access shall be available to staff as a tool by which to provide, exchange, and retrieve information and documents for use in the performance of necessary job functions.

**RELATED POLICIES:**

01.04.105 Use of Department Computer Equipment, Software and Services  
State of Michigan Technical Standard 1340.00.130.02 Acceptable Use of Information Technology

**POLICY:**

GENERAL INFORMATION

- A. The Department of Technology, Management and Budget (DTMB) is responsible for identifying software authorized to be used by State of Michigan employees to access the internet on a Department computer. Only software approved by DTMB shall be installed and used.
- B. Staff shall access the internet in accordance with PD 01.04.105 "Use of Department Computer Equipment, Software and Services" and State of Michigan Technical Standard 1340.00.130.02 Acceptable Use of Information Technology.
- C. Department computers located within the secure perimeter of a correctional facility shall have internet access only as authorized by this policy. However, a laptop or other device that can access the internet may be brought inside the security perimeter with approval from the Deputy Director or designee provided the device is not otherwise prohibited within the facility. Cellular telephones that can access the internet may be brought inside the security perimeter only as set forth in PD 04.04.100 "Custody, Security, and Safety Systems (Exempt)." A device with internet access that is approved to be brought inside the security perimeter may be used only to access those internet sites to which all State of Michigan employees have access or as otherwise approved by the Deputy Director. This is not intended to prohibit use of the device for word processing or e-mail or in other ways unrelated to internet access.
- D. Computers with internet access shall be located only in areas that are not accessible to prisoners, probationers, and parolees unless the offender is in the area under direct staff supervision. A prisoner shall not be permitted to use a computer that has internet access except with the approval of the Deputy Director after consultation with the Agency Security Officer. Approval shall be granted only to access internet-based programs and services that are consistent with programming objectives (e.g., educational programming; job training) and efficient operations, and that do not pose a threat to the safety and security of the facility. A probationer or parolee under supervision in the community shall not be permitted to use a Department computer that has internet access.

APPROVAL PROCESS

- E. All staff assigned a Department computer are pre-approved to have internet access to websites within web categories to be accessed by all State of Michigan employees. The appropriate supervisor may authorize expanded internet access based on the duties of the position, however, requests for positions located within the secure perimeter of a correctional facility may be approved only if access is necessary to perform the primary work responsibilities assigned to the position. An Internet Access Exception Request (DTMB-0099) shall be used to request and approve expanded internet access, and the request may be denied at any level. The DTMB-0099 can be found on the DTMB forms website. If the DTMB-0099 is approved, the Agency Security Officer shall submit a Remedy incident with documentation attached to the Michigan Security

DOCUMENT TYPE POLICY DIRECTIVE	EFFECTIVE DATE 08/23/2021	NUMBER 01.04.104	PAGE 2 OF 2
-----------------------------------	------------------------------	---------------------	-------------

Operations Center (MiSOC) to give the approved employee expanded internet access.

- F. The Agency Security Officer shall ensure that a current list of all Department positions approved to have expanded internet access is maintained.

#### MONITORING INTERNET ACTIVITIES

- G. Users have no expectation of privacy in their use of State of Michigan-provided intranet or internet access, or other State of Michigan information systems. The State of Michigan actively monitors information technology (IT) resources to ensure compliance with policy. This includes real-time monitoring of network traffic; the transfer of data created, sent, received, or stored on IT resources, and other monitoring and auditing the State of Michigan may deem necessary. The State of Michigan also blocks unauthorized internal and external traffic and services that may cause risk to IT resources. If there is any evidence of illegal activity or unacceptable use discovered during monitoring or reviews, the Agency Security Officer shall ensure that this information is reported to the Internal Affairs Section.
- H. An employee's internet activities also may be monitored upon request of the facility head, Field Operations Administration (FOA) Assistant Deputy Director (ADD) or designee, Correctional Facilities Administration (CFA) ADD, or, for Central Office, other appropriate Administrator if it is believed that the employee may be using the internet or accessing websites for unauthorized reasons. Such requests are subject to approval of the Budget and Operations Administration (BOA) Deputy Director or designee and shall be submitted through MDOC Human Resource Department using a Request to Monitor Usage of Information Technology Resources form (DTMB-130). If approved by the BOA Deputy Director, Agency Security Officer shall forward the request to DTMB to initiate the monitoring process. DTMB will send a written report to Agency Security Officer for forwarding to the requestor upon completion of the requested monitoring period.

#### ACCESS FOR NON-DEPARTMENT EMPLOYEES

- I. Contractual employees and other non-Department employees who provide services at a Department facility or office may be approved by the appropriate Executive Policy Team (EPT) member or designee to use a Department computer with internet access for authorized purposes. If approved, the non-Department employee shall be given a copy of this policy directive and required to verify receipt in writing prior to being allowed to access the internet. A violation of the security requirements set forth in this policy shall result in termination of the non-Department employee's access to the internet.
- J. If a contractual employee or other non-Department employee has access to the internet through their personal computer and wants to connect to the internet at the facility or office Local Area Network (LAN), the facility head or office supervisor may approve such access in accordance with this policy. If approved, the non-Department employee shall be given a copy of this policy directive and required to verify receipt in writing prior to being allowed to access the internet. A violation of the security requirements set forth in this policy shall result in termination of the non-Department employee's access to the LAN.

#### PROCEDURES

- K. If necessary, to implement requirements set forth in this policy directive, Wardens, the FOA Deputy Director, and the Agency Security Officer shall ensure that procedures are developed or updated.

#### AUDIT ELEMENTS

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

APPROVED: HEW 06/28/2021