MICHIGAN DEPARTMENT OF CORRECTIONS **POLICY DIRECTIVE**	EFFECTIVE DATE 12/01/11	NUMBER 01.04.104
SUBJECT INTERNET ACCESS	SUPERSEDES 01.04.104 (04/14/10)	
	AUTHORITY MCL 791.203; Annual Appropriations Act	
	ACA STANDARDS 4-4100, 4-4101, 4-4102, 4-ACRS-7D-05, 4-ACRS-7D-06, 1-ABC-1F-01, 1-ABC-1F-02, 1-ABC-1F-04	
	PAGE 1 OF 3	

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

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 only as needed in the performance of their job responsibilities and in accordance with PD 01.04.105 "Use of Department Computer Equipment, Software and Services".

C. Department computers located within the security perimeter of a Correctional Facilities Administration (CFA) institution or Field Operations Administration (FOA) 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 appropriate 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". 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, or any offender in a Department facility, shall not be permitted to use a computer which has internet access except with approval of the CFA or FOA Deputy Director after consultation with the Manager of the Automated Data Systems Section (ADSS), Operations Support Administration (OSA). 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 which 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 which has internet access.

MICHIGAN INFORMATION TECHNOLOGY EXECUTIVE COUNCIL

E. The Michigan Information Technology Executive Council is an advisory board comprised of

representatives from each State department. Included in the Council's responsibilities is the authority to define and approve which website categories (e.g., government; news and media) all State of Michigan employees may access. The Council also is responsible for identifying additional website categories to which employees may have access based on the duties of the employee's position; this expanded access is allowed only as set forth in this policy directive.

APPROVAL PROCESS

F. All staff assigned a Department computer are pre-approved to have internet access to websites within web categories approved by the Michigan Information Technology Executive Council to be accessed by all State of Michigan employees. The appropriate Executive Policy Team (EPT) member may authorize expanded internet access based on the duties of the position; however, requests for positions located within the security perimeter of a CFA institution or FOA facility may be approved only if access is necessary to perform the primary work responsibilities assigned to the position. An Internet Access Exception Request (DIT-0099) shall be used to request and approve expanded internet access; the request may be denied at any level.

G. Whenever an EPT member approves expanded internet access for an employee in an approved position, the EPT member shall ensure that the Approved Internet Access Exception Request (DIT-0099) is sent to DTMB to allow for access to the expanded websites; a copy also shall be sent to appropriate supervisors and ADSS as notification of the approval. If the approval for the position to have expanded internet is subsequently withdrawn or modified, the EPT member shall ensure that ADSS and DTMB is notified using the Approved Internet Access Exception Request (DIT-0099) so that DTMB may close access to the expanded sites as needed. The EPT member shall similarly notify DTMB whenever an employee in a position approved to have expanded internet transfers to a position not authorized to have the same expanded access. Notifications to ADSS and DTMB shall be on an Approved Internet Access Exception Request form (DIT-0099).

H. The ADSS Manager shall ensure that a current list of all Department positions approved to have expanded internet access is maintained.

MONITORING INTERNET ACTIVITIES

I. All employees are subject to routine monitoring of their internet activities. If the monitoring reveals any suspicious internet activity by an employee, the ADSS Manager shall ensure that this information is reported to the appropriate supervisor.

J. An employee's internet activities also may be monitored upon request of the facility head, FOA Regional Administrator or designee, Regional Prison Administrator, or, for Central Office, other appropriate Administrator if it is believed that the employee may be using the internet or accessing websites for reasons unrelated to the performance of his/her job responsibilities. Such requests are subject to approval of the OSA Deputy Director or designee and shall be submitted through ADSS using a Request to Monitor Usage of Information Technology Resources form (DIT-130). If approved by the OSA Deputy Director, ADSS shall forward the request to DTMB to initiate the monitoring process. DTMB will send a written report to ADSS for forwarding to the requestor upon completion of the requested monitoring period.

ACCESS FOR NON-DEPARTMENT EMPLOYEES

K. Contractual employees and other non-Department employees who provide services at a Department facility or office may be approved by the appropriate EPT member or designee to use a Department computer with internet access for official business associated with the services provided. 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.

L. If a contractual employee or other non-Department employee has access to the internet through his/her personal computer and wants to connect to the internet at the facility or office Local Area Network (LAN) for official business associated with the services provided to the Department, 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

M. Wardens, the FOA Deputy Director, and the ADSS Manager shall ensure that procedures are developed as necessary to implement requirements set forth in this policy directive. Procedures shall be completed within 60 calendar days after the effective date of this policy directive. This includes ensuring that their existing procedures are revised or rescinded, as appropriate, if inconsistent with policy requirements or no longer needed.

AUDIT ELEMENTS

N. 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 Audit of Policies and Procedures”.

APPROVED: DHH 12/01/11