	<b>State of Michigan</b> <b>Department of Information Technology</b> <b>POLICY AND PROCEDURE MANUAL</b>	<b>TYPE</b> <b>Policy/Procedure</b>
		<b>NUMBER</b> <b>200.25</b>
		<b>PAGE</b> <b>1 of 4</b>

<b>SUBJECT</b> <b>IT Violations to Acceptable Use Policy</b>	<b>EFFECTIVE DATE</b> <b>4/25/05</b>
---	---

**Policy**

The purpose of this policy is to outline and clarify the range of potential consequences for violating enterprise security, telecommunications, computing, and acceptable use policies outlined in department policies and in the DMB Administrative Guide 1300 and 1400 series.

DIT may take disciplinary action, up to an including dismissal for violations of this policy.

**Persons, Groups, and Systems Affected**

All DIT employees utilizing any State of Michigan computing, data, telecommunications resources, or MPSCS communications resources are affected by this policy.

DIT authorizes, controls, and reserves the right to grant any employee access to computing, data, MPSCS communications, or telecommunications resources.

All employees using computing, data, MPSCS communications, and telecommunications resources are required to be familiar with acceptable use policies, security and privacy protection policies, and general telecommunications, computer system, and data resource policies applicable in their work environment. Front line supervisors, managers, and directors all share in the responsibility for maintaining policy awareness within their employee groups.

**General Information**


**Activities that may result in disciplinary action**

No list can contain all of the behaviors and performance issues that may prompt disciplinary action. The lists contained in this section are intended to provide an understanding of the response the department anticipates taking for these and/or similar offenses. Repeated offenses and other aggravating situations or conditions can lead to a more severe disciplinary action than is shown here.

**Disciplinary Guide – Types of Offenses**

**Type One** – The following types of offenses may subject an employee to a formal reprimand for the first offense. Multiple concurrent offenses or repeat offenses in one year becomes a Type Two and may be cause for a suspension and/or unsatisfactory interim performance rating. This list is not all-inclusive.

1. Pirated software – downloading: willful possession on a state computer of software in violation of copyright law. For example, not legally purchased, provided in violation of copyright law or that has been intentionally modified to circumvent copy protection.
2. Downloading movies, freeware, and or games: misuse of state resources to acquire and/or store files of entertainment value only, material inappropriate for business or professional use.

 <p>MICHIGAN DEPARTMENT OF  <b>dit</b>  INFORMATION TECHNOLOGY</p>	<p>State of Michigan  Department of Information Technology  <b>POLICY AND PROCEDURE MANUAL</b></p>	<table border="1"> <tr> <td>TYPE</td> <td>Policy/Procedure</td> </tr> <tr> <td>NUMBER</td> <td>200.25</td> </tr> <tr> <td>PAGE</td> <td>2 of 4</td> </tr> </table>	TYPE	Policy/Procedure	NUMBER	200.25	PAGE	2 of 4
TYPE	Policy/Procedure							
NUMBER	200.25							
PAGE	2 of 4							
<p>SUBJECT  <b>IT Violations to Acceptable Use Policy</b></p>		<p>EFFECTIVE DATE  <b>4/25/05</b></p>						
<ol style="list-style-type: none"> <li>3. Sharing access codes: giving a user ID and password or other identifying artifacts for accessing the State's information network/computers to an unauthorized individual(s).</li> <li>4. Compromising the privacy or integrity of confidential data.</li> <li>5. Online gambling or gaming: use of IT resources to participate in games of chance that offer monetary or items of value as a reward. Participating in the electronic equivalent of games. (For example: poker, chess, and monopoly.)</li> <li>6. Uploading or transferring source code to unauthorized person(s)/company(s).</li> <li>7. Willfully sending, receiving, downloading, displaying, printing, or otherwise gaining access to material that is sexually explicit, obscene, threatening, defamatory, fraudulent, false, harassing, racist, or discriminatory.</li> <li>8. Use of state resources to knowingly misrepresent ones identity for illegal or inappropriate activity.</li> <li>9. Sending, receiving, downloading or otherwise disseminate software, macros and data files that are known to a contain virus, malicious program code or self-replicating code.</li> </ol> <p>Note: An appeal of a written reprimand is filed at Step One of the grievance procedure or with the immediate supervisor.</p> <p><b>Type Two</b> – Any of the following types of violations may subject an employee to a suspension and/or an unsatisfactory interim performance rating for the first offense. Multiple concurrent offenses or a repeat offense within two years becomes a Type Three violation and may be cause for discharge.</p> <p>Willfully providing to others or disseminating material that is sexually explicit, obscene, threatening, defamatory, fraudulent, false, harassing, and racist, discriminatory or otherwise illegal or unlawful.</p> <ol style="list-style-type: none"> <li>1. Pirated software – distributing or providing to others software in violation of copyright law. For example, files or codes not legally purchased.</li> <li>2. Creating, maintaining or updating computer infrastructure from or on State of Michigan IT resources for purposes not related to state business.</li> <li>3. Visiting of known hacker's websites, acquiring and storing of hacker tools. Hacker software is a general term used to describe software designed to bypass security, obtain confidential electronic information, and subvert security structures in place to protect state property/resources, individual privacy and to circumvent copy protection.</li> <li>4. Electronic harassment: use of state IT infrastructure for any activity defined as harassment.</li> </ol>								

5. Transmitting confidential state/client information: any willful violation of laws or policy published by the State of Michigan or the employees' managerial structure governing the confidentiality of state or personal information through the use of IT resources.

Note: All appeals of suspensions are to be filed directly with the Employee Relations Section, Office of Human Resources. Appeals of unsatisfactory interim performance ratings are to be filed at Step One of the grievance procedure or with the immediate supervisor.

**Type Three** – The following types of offenses may subject an employee to immediate discharge.

1. Child pornography: willful access or possession of material defined as child pornography by federal or state law.
2. Destructive practices or behavior: willful destruction of property or information, i.e., state computer files/data/source code or resources.
3. Hacking: willful illegal access to computer or data.
4. Any computer-aided felony conviction.

Note: All appeals of dismissals are to be filed directly with the Labor Relations Section, Office of Human Resources.

**Procedures**

<b>Responsibility</b>	<b>Action</b>
DIT Employee	<ol style="list-style-type: none"> <li>1. Identifies suspected violation.</li> <li>2. Reports to supervisor.</li> </ol>
DIT Supervisor	<ol style="list-style-type: none"> <li>3. Reports suspected violation to Employee Services.</li> </ol>
Employee Services	<ol style="list-style-type: none"> <li>4. Requests/authorizes investigation with Office of Enterprise Security.</li> </ol>



State of Michigan  
Department of Information Technology  
**POLICY AND PROCEDURE MANUAL**

TYPE  
**Policy/Procedure**

NUMBER  
**200.25**

PAGE  
**4 of 4**

SUBJECT  
**IT Violations to Acceptable Use Policy**

EFFECTIVE DATE  
**4/25/05**

Office of Enterprise Security	5. Conducts acceptable use investigation. 6. Reports results to Employee Services.
Employee Services	7. Consults with Labor Relations and supervisor to determine applicable disciplinary action. 8. Implements disciplinary process as applicable.

**Reference**

DIT Acceptable Use Policy  
DMB's Administrative Guide 1300 and 1400 series  
Civil Service Rule 2-6

**Contact/Update Responsibility**

Any questions or concerns regarding this policy should be directed to DIT Employee Services.

**Approving Authority**

Teri Takai, Director: *(signed by Director Takai)*      Date: *(4/25/05)*