



**DEPARTMENT OF ENVIRONMENTAL QUALITY  
POLICY AND PROCEDURES**

**SUBJECT: TELECOMMUNICATION DEVICE  
ACCEPTABLE USE POLICY**

**Number: 02-001**

**Date: November 18, 1997  
Revised April 29, 2002  
Revised November 4, 2005**

**Page 1 of 5**

**<<ISSUE>>**

Acceptable use of telecommunication devices in the Department of Environmental Quality (DEQ) is essential.

DEQ employees use a number of telecommunication devices, provided by the DEQ or the State, to communicate within the DEQ, with other government agencies, with customers and stakeholders, and with the general public. These devices include, but are not necessarily limited to, computers, modems, telephones, cellular telephones, voice mail, two-way radios, and telefaxes. The purpose of these devices is to facilitate the DEQ's ability to conduct its business, administer regulations, and achieve its mission. Although they are essential, the accessibility of these tools to all employees at almost any time and place and for any reason dictates that the DEQ set forth guidelines and policies regarding their acceptable use.

The Department of Management and Budget (DMB) has recognized some of the challenges and issues surrounding the acceptable use of telecommunication devices in State government and has accordingly developed policies for their use (DMB Procedures 1210.13, 1410.14 and 1460). All users of State telecommunication network devices must comply with these policies.

There are, however, some additional issues specific to the DEQ use of telecommunication devices which are not fully addressed in the DMB policies. Some of these issues include monitoring of telecommunication devices by DEQ management, proper representation of the DEQ by employees using telecommunication devices (particularly electronic mail), for Internet use (see DEQ Internet Usage Policy 02-002), and incurring long distance or other telephone charges.

**<<DEFINITIONS>>**

None.

**<<STATEMENT OF POLICY>>**

The DEQ supports employee use of its telecommunication devices which is done in compliance with State Law (Public Act 53 of 1979), Civil Service Rules 1-13 and 1-14, and DMB Procedures 1210.13, 1410.14 and 1460. The DEQ desires that its policy on this subject conform to State Law (Public Act 53 of 1979), Civil Service Rules 1-13 and 1-14, and DMB Procedures 1210.13, 1410.14 and 1460, and they are hereby incorporated into this policy and included as part of Attachment A.

## DEQ POLICY AND PROCEDURES

**SUBJECT: TELECOMMUNICATION DEVICE  
ACCEPTABLE USE POLICY**

**Number: 02-001**

**DATE: November 18, 1997  
Revised April 29, 2002  
Revised November 4, 2005**

**Page 2 of 5**

In recognition of the additional specific issues regarding DEQ employees' use of telecommunication devices, the DEQ policy is as follows:

- 1. Professional Demeanor:** Employee use of all workplace telecommunication devices must reflect a professional demeanor. An employee may not use a workplace telecommunication device to create, store, retrieve, or transfer information that contains unprofessional content such as profanity, vulgarity, or discriminatory statements.
- 2. Freedom of Information Act and Telecommunication:** Employees should be aware that all information stored electronically on workplace equipment is subject to the provisions of the Freedom of Information Act except where it is specifically exempted by the Act.
- 3. Sending Electronic Mail (e-mail) to Entities Outside the DEQ:** A message sent by means of e-mail to entities outside the DEQ must be written and prepared using the same quality assurance and management oversight as a message sent on DEQ letterhead. An employee may generate e-mail only for purposes directly related to the employee's job duties. Supervisors must provide guidance to their employees regarding how e-mail should be used in the performance of employees' job responsibilities. Included in this guidance should be examples of entities with whom the employee may communicate by e-mail, the examples of the normal nature of such communications, examples of instances in which the employee should seek supervisory review and assistance with e-mail messages, and examples of instances in which the employee should not use e-mail.
- 4. Monitoring Employee Use of Telecommunication Devices:** Employees should be aware that use of State and DEQ telecommunication devices may be monitored by the Department of Information Technology (DIT) or the DEQ. An employee should have no expectation of privacy in the use of these devices. The DEQ may monitor employee Internet activities to ensure compliance with the DEQ Internet Usage Policy.
- 5. Activities Which Incur Long Distance or other Telephone Charges:** An employee may incur a DEQ long distance telephone charge only in the performance of work-related duties. An employee may not make a personal long distance telephone call which will be charged to the DEQ's long distance telephone bill, except as necessary to communicate unavoidable delays in scheduled work departure times, or to communicate unavoidable change in travel plans while in travel status. Also, an employee may not use any other telecommunication device

## DEQ POLICY AND PROCEDURES

**SUBJECT: TELECOMMUNICATION DEVICE  
ACCEPTABLE USE POLICY**

**Number: 02-001**

**DATE: November 18, 1997  
Revised April 29, 2002  
Revised November 4, 2005**

**Page 3 of 5**

(such as a telefax, modem, or cellular telephone) for personal use which will generate a charge to the DEQ telephone bill.

6. **Acceptable Use Form:** New employees must read and sign the DEQ "Telecommunication Device Acceptable Use Agreement" form (Attachment B) prior to being issued or authorized to use DEQ telecommunication devices.
7. **Disciplinary Action:** Employees should understand that noncompliance with State Law (Public Act 53 of 1979), Civil Service Rules 1-13 and 1-14, DMB Procedures 1210.13, 1410.14 and 1460, or this policy may result in disciplinary action in accordance with applicable union contracts and Civil Service Rules, up to and including dismissal from State employment.

### **PROCEDURE A: Authorization to Send E-Mail Messages to Entities Outside the DEQ.**

#### **Responsibility**

#### **Action**

Supervisor

1. Provides guidance to each employee regarding that employee's authorized use of e-mail and the Internet, including the issues specified in policy criteria 3 and 4.
2. Provides guidance to each employee on utilizing e-mail.

### **PROCEDURE B: DEQ Monitoring of Employee Telecommunication Devices**

#### **Responsibility**

#### **Action**

Supervisor

1. Requests available information about employee use of telecommunication device through chain of command to Division/Office Chief, with reason(s) for the request and a time duration.

Division/Office Chief

2. Evaluates request.
  - A. If approved, forwards request to appropriate Deputy Director with cover memorandum outlining reason(s) for request and a time duration.

**DEQ POLICY AND PROCEDURES**

**SUBJECT: TELECOMMUNICATION DEVICE  
ACCEPTABLE USE POLICY**

**Number: 02-001**

**DATE: November 18, 1997  
Revised April 29, 2002  
Revised November 4, 2005**

**Page 4 of 5**

**PROCEDURE B: DEQ Monitoring of Employee Telecommunication Devices,**  
continued

- B. If denied, returns request to originating supervisor through chain of command with reason(s) for denial.
  
- 3. Evaluates request received from Division/Office Chief.
  - A. If approved and if information is available from the DIT, obtains relevant information.
  - B. If approved but information is not available from the DIT, returns request to Division/Office Chief advising that such information is not available.
  - C. If denied, returns request to Division/Office Chief advising of reason(s) for denial.
  
- 4. Provides telecommunication device usage information requested in Step 3.A.
  
- 5. Reviews information received from the DIT with Division/Office Chief to determine appropriate action. If disciplinary action is necessary, contacts the Office of Human Resources (OHR). Works with OHR to take appropriate action.

**PROCEDURE C: Obtaining Employee Signature on DEQ Telecommunication Device Acceptable Use Form**

**Responsibility**

**Action**

Office of Human Resources

- 1. Provides Telecommunication Device Acceptable Use Agreement form EQ 1217E (Attachment B) to employees:
  - A. New Employee - Provides Telecommunication Device Acceptable Use Agreement form EQ 1217E to new employee with other forms to be signed

**DEQ POLICY AND PROCEDURES**

**SUBJECT: TELECOMMUNICATION DEVICE  
ACCEPTABLE USE POLICY**

**Number: 02-001**

**DATE: November 18, 1997  
Revised April 29, 2002  
Revised November 4, 2005**

**Page 5 of 5**

**PROCEDURE C: DEQ Monitoring of Employee Telecommunication Devices,**  
continued

during New Employee Orientation, along with Public Act 53 of 1979, Civil Service Rules 1-13 and 1-14, DMB Procedures 1210.13, 1410.14 and 1460 (collectively, Attachment A).

B. Existing Employee - Provides Telecommunication Device Acceptable Use Agreement form EQ 1217E to existing employee along with Public Act 53 of 1979, Civil Service Rules 1-13 and 1-14, DMB Procedures 1210.13, 1410.14 and 1460 (collectively, Attachment A).

New and Existing Employee

2. Reads Public Act 53 of 1979, Civil Service Rules 1-13 and 1-14, DMB Procedures 1210.13, 1410.14 and 1460 (collectively, Attachment A). Signs form and returns it to Office of Human Resources during New Employee Orientation (for a new employee) or within 90 days of effective date of policy (for an existing employee).

Office of Human Resources

3. Places signed form in Department employee personnel file.

---

Approved: \_\_\_\_\_ Date: \_\_\_\_\_

## ATTACHMENT A

### I. PUBLIC ACT 53 OF 1979 as amended

#### 752.791 Meanings of words and phrases.

Sec. 1. For the purposes of this act, the words and phrases defined in sections 2 and 3 have the meanings ascribed to them in those sections.

**History:** 1979, Act 53, Eff. Mar. 27, 1980.

#### FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.792 THIS SECTION IS AMENDED EFFECTIVE APRIL 1, 1997: See  
752.792.amended \*\*\*\*\*

#### 752.792 Definitions; A to D.

Sec. 2. (1) "Access" means to instruct, communicate with, store data in, retrieve or intercept data from, or otherwise use the resources of a computer program, computer, computer system, or computer network.

(2) "Aggregate amount" means any direct or indirect loss incurred by a victim including, but not limited to, the value of any money, property or service lost, stolen, or rendered unrecoverable by the offense, or any actual expenditure incurred by the victim to verify that a computer program, computer, computer system, or computer network was not altered, acquired, damaged, deleted, disrupted, or destroyed by the access.

(3) "Computer" means any connected, directly interoperable or interactive device, equipment, or facility that uses a computer program or other instructions to perform specific operations including logical, arithmetic, or memory functions with or on computer data or a computer program and that can store, retrieve, alter, or communicate the results of the operations to a person, computer program, computer, computer system, or computer network.

(4) "Computer network" means the interconnection of hardwire or wireless communication lines with a computer through remote terminals, or a complex consisting of 2 or more interconnected computers.

(5) "Computer program" means a series of internal or external instructions communicated in a form acceptable to a computer that directs the functioning of a computer, computer system, or computer network in a manner designed to provide or produce products or results from the computer, computer system, or computer network.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, software, or hardware.

(7) "Device" includes, but is not limited to, an electronic, magnetic, electrochemical, biochemical, hydraulic, optical, or organic object that performs input, output, or storage functions by the manipulation of electronic, magnetic, or other impulses.

**History:** 1979, Act 53, Eff. Mar. 27, 1980;--Am. 1996, Act 326, Eff. Apr. 1, 1997.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.793 THIS SECTION IS AMENDED EFFECTIVE APRIL 1, 1997: See  
752.793.amended \*\*\*\*\*

**752.793 Definitions; P to S.**

Sec. 3. (1) "Property" includes financial instruments; information, including electronically produced data; computer software and programs in either machine or human readable form; and any other tangible or intangible item of value.

(2) "Services" includes computer time, data processing, and storage functions.

**History:** 1979, Act 53, Eff. Mar. 27, 1980.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.793.amended THIS AMENDED SECTION IS EFFECTIVE APRIL 1, 1997  
\*\*\*\*\*

**752.793 Definitions; P to S.**

Sec. 3. (1) "Property" includes, but is not limited to, intellectual property, computer data, instructions or programs in either machine or human readable form, financial instruments or information, medical information, restricted personal information, or any other tangible or intangible item of value.

(2) "Services" includes, but is not limited to, computer time, data processing, storage functions, computer memory, or the unauthorized use of a computer program, computer, computer system, or computer network, or communication facilities connected or related to a computer, computer system, or computer network.

**History:** 1979, Act 53, Eff. Mar. 27, 1980;--Am. 1996, Act 326, Eff. Apr. 1, 1997.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.794 THIS SECTION IS AMENDED EFFECTIVE APRIL 1, 1997: See  
752.794.amended \*\*\*\*\*

**752.794 Prohibited access to computer, computer system, or computer network.**

Sec. 4. A person shall not, for the purpose of devising or executing a scheme or artifice with intent to defraud or for the purpose of obtaining money, property, or a service by means of a false or fraudulent pretense, representation, or promise with intent to, gain access to or cause access to be made to a computer, computer system, or computer network.

**History:** 1979, Act 53, Eff. Mar. 27, 1980.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.794.amended THIS AMENDED SECTION IS EFFECTIVE APRIL 1, 1997  
\*\*\*\*\*

**752.794 Prohibited access to computer program, computer, computer system, or computer network.**

Sec. 4. A person shall not intentionally access or cause access to be made to a computer program, computer, computer system, or computer network to devise or execute a scheme or artifice with the intent to defraud or to obtain money, property, or a service by a false or fraudulent pretense, representation, or promise.

**History:** 1979, Act 53, Eff. Mar. 27, 1980;--Am. 1996, Act 326, Eff. Apr. 1, 1997.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.795 THIS SECTION IS AMENDED EFFECTIVE APRIL 1, 1997: See  
752.795.amended \*\*\*\*\*

**752.795 Gaining access to, altering, damaging, or destroying computer, computer system or network, software program, or data.**

Sec. 5. A person shall not intentionally and without authorization, gain access to, alter, damage, or destroy a computer, computer system, or computer network, or gain access to, alter, damage, or destroy a computer software program or data contained in a computer, computer system, or computer network.

**History:** 1979, Act 53, Eff. Mar. 27, 1980.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.795.amended THIS AMENDED SECTION IS EFFECTIVE APRIL 1, 1997  
\*\*\*\*\*

**752.795 Prohibited conduct.**

Sec. 5. A person shall not intentionally and without authorization or by exceeding valid authorization do any of the following:

(a) Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.

(b) Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network. This subdivision does not prohibit conduct protected under section 5 of article I of the state constitution of 1963 or under the first amendment of the constitution of the United States.

**History:** 1979, Act 53, Eff. Mar. 27, 1980;--Am. 1996, Act 326, Eff. Apr. 1, 1997.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.796 THIS SECTION IS AMENDED EFFECTIVE APRIL 1, 1997: See  
752.796.amended \*\*\*\*\*

**752.796 Violations.**

Sec. 6. A person shall not utilize a computer, computer system, or computer network to commit a violation of section 174 of Act

No. 328 of the Public Acts of 1931, as amended, being section 750.174 of the Michigan Compiled Laws, section 279 of Act No. 328 of the Public Acts of 1931, being section 750.279 of the Michigan Compiled Laws, section 356 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.356 of the Michigan Compiled Laws, or section 362 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.362 of the Michigan Compiled Laws.

**History:** 1979, Act 53, Eff. Mar. 27, 1980.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.796.amended THIS AMENDED SECTION IS EFFECTIVE APRIL 1, 1997  
\*\*\*\*\*

**752.796 Use of computer program, computer, computer system, or computer network to commit crime.**

Sec. 6. A person shall not utilize a computer program, computer, computer system, or computer network to commit a crime.

**History:** 1979, Act 53, Eff. Mar. 27, 1980;--Am. 1996, Act 326, Eff. Apr. 1, 1997.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.797 THIS SECTION IS AMENDED EFFECTIVE APRIL 1, 1997: See  
752.797.amended \*\*\*\*\*

**752.797 Penalties.**

Sec. 7. A person who violates this act, if the violation involves \$100.00 or less, is guilty of a misdemeanor. If the violation involves more than \$100.00, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of not more than \$5,000.00, or both.

**History:** 1979, Act 53, Eff. Mar. 27, 1980.

FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND  
COMPUTER NETWORKS (Act 53 of 1979)

\*\*\*\*\* 752.797.amended THIS AMENDED SECTION IS EFFECTIVE APRIL 1, 1997  
\*\*\*\*\*

**752.797 Penalties; prior convictions; presumption.**

Sec. 7. (1) A person who violates this act is guilty of a crime as follows:

(a) If the violation involves an aggregate amount of less than \$200.00, the person is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than

\$500.00 or 3 times the aggregate amount, whichever is greater, or both imprisonment and a fine.

(b) If any of the following apply, the person is guilty of a misdemeanor punishable by imprisonment for not more than 1 year or a fine of not more than \$2,000.00 or 3 times the aggregate amount, whichever is greater, or both imprisonment and a fine:

(i) The violation involves an aggregate amount of \$200.00 or more but less than \$1,000.00.

(ii) The person violates this act and has a prior conviction for committing or attempting to commit a violation of this act.

(c) If any of the following apply, the person is guilty of a felony punishable by imprisonment for not more than 5 years or a fine of not more than \$10,000.00 or 3 times the aggregate amount, whichever is greater, or both imprisonment and a fine:

(i) The violation involves an aggregate amount of \$1,000.00 or more but less than \$20,000.00.

(ii) The person violates this act and has 2 prior convictions for violating this act.

(d) If any of the following apply, the person is guilty of a felony punishable by imprisonment for not more than 10 years or a fine of not more than 3 times the aggregate amount, or both imprisonment and a fine:

(i) The violation involves an aggregate amount of \$20,000.00 or more.

(ii) The person violates this act and has 3 or more prior convictions for violating this act.

(2) If the prosecuting attorney intends to seek an enhanced sentence based upon the defendant having a prior conviction, the prosecuting attorney shall include on the complaint and information a statement listing that prior conviction. The existence of the defendant's prior conviction shall be determined by the court, without a jury, at sentencing. The existence of a prior conviction may be established by any evidence relevant for that purpose, including, but not limited to, 1 or more of the following:

(a) A copy of the judgment of conviction.

(b) A transcript of a prior trial, plea-taking, or sentencing.

(c) Information contained in a presentence report.

(d) The defendant's statement.

(3) It is a rebuttable presumption that the person did not have authorization from the owner, system operator, or other person who has authority from the owner or system operator to grant permission to access the computer program, computer, computer system, or computer network or has exceeded authorization unless 1 or more of the following circumstances existed at the time of access:

(a) Written or oral permission was granted by the owner, system operator, or other person who has authority from the owner or system operator to grant permission of the accessed computer program, computer, computer system, or computer network.

(b) The accessed computer program, computer, computer system, or computer network had a pre-programmed access procedure that would display a bulletin, command, or other message before access was achieved that a reasonable person would believe identified the computer program, computer, computer system, or computer network as within the public domain.

(c) Access was achieved without the use of a set of instructions, code, or computer program that bypasses, defrauds, or otherwise circumvents the pre-programmed access procedure for the computer program, computer, computer system, or computer network.

**History:** 1979, Act 53, Eff. Mar. 27, 1980;--Am. 1996, Act 326, Eff. Apr. 1, 1997.II.

## Civil Services Rules. 1-13 & 1-14

### Section 13

#### Patents – Inventions

1-13.1 Employee Rights. — The property rights in a patent on an invention created by an employee are subject to contract entered into by the state administrative board as provided by law. The employee's compensation is fifteen (15) percent of the net royalties which may result from the invention. The compensation provisions of this rule are non-negotiable. However, any dispute concerning the employee's property rights relative to the state's property rights in such an invention is grievable.

1-13.2 Grants and Contracts. — This rule does not preclude the acceptance of grants or contracts under provisions of applicable federal laws or regulations that require a different disposition of patents or right thereof to obtain patents.

---

### Section 1-14

#### Copyrights

1-14.1 Employee Rights. — The property rights in a copyright that subsists in a work created by a classified employee as an author-employee belong to the state and are subject to contract entered into by the state administrative board as provided by law. The author-employee's compensation is fifteen (15) percent of the net royalties from written licenses or transfers to third parties by the state of Michigan that may result from a work, but only when the state or agency has obtained a certificate of copyright. The compensation provisions of this rule are not negotiable. However, any dispute concerning the author-employee's property rights relative to the state's property rights in such a copyright is grievable.

1-14.2 Grants and Contracts. — This rule does not preclude the acceptance of grants or contracts under provisions of applicable federal laws or regulations that require a different disposition of the copyright in works.

III. DMB PROCEDURE 1210.13  
Issued August 5, 1996

SUBJECT: Usage of the State telephone system by State employees.

APPLICATION: Executive Branch Departments and Sub-units.

PURPOSE: To establish statewide policy and procedures governing employee use of the State telephone system and State issued telephone credit cards.

CONTACT AGENCY: Department of Management and Budget (DMB) - Office of Financial Management (OFM).

TELEPHONE: 517/373-1010

FAX: 517/373-6458

SUMMARY: State employees should use the State telephone system and State issued telephone credit cards only to conduct official State business.

State employees are prohibited from utilizing the State telephone system or a State issued telephone credit card to place personal long distance telephone calls, except as necessary to communicate unavoidable delays in scheduled work departure times, or to communicate unavoidable change in travel plans while in travel status, or as authorized by their supervisor based upon the circumstances involved.

Use of State telephones for personal local calls should be kept to a minimum.

Each department/agency is responsible for ensuring that its employees understand and comply with this policy on appropriate telephone usage. Although not required, agencies may utilize a written employee certification as a possible means to ensure that this policy is understood (see example - Exhibit A). If used, such certification should be maintained in the employee's personnel file at the agency where employed.

Notwithstanding the basic provisions of this procedure, any charges for telephone calls placed for personal purposes, along with applicable state and federal taxes, must be collected from the individual who placed the call. For reimbursements received during the same fiscal year in which the charge was paid by the State, an expenditure credit should be processed. All others should be credited to a miscellaneous revenue account.

Although detailed validation of telephone billings and maintenance of telephone usage logs are not required, state agencies should utilize

review processes, appropriate for the circumstances, to monitor compliance with this policy and procedure.

As part of the overall process of reviewing telephone billings for approval prior to payment, local and long distance telephone charges should be reviewed by agency supervisory personnel or the department administrative/finance office for unusual usage prior to billing approval. Any suspected misuse that violates this policy and procedure should be investigated and, if such misuse persists, appropriate corrective action should be taken.

Agency internal auditors should include periodic review of compliance with this policy and procedure in their annual audit plans.

Whenever possible and cost effective, state agencies should consider placing software restriction on telephone lines to disable the ability to make long distance calls from work stations where there is no legitimate business need to make such calls.

APPLICABLE FORMS: Exhibit A - Suggested format for employee certification

PROCEDURES:

Employees:

- May be required to sign a certification acknowledging their understanding of this telephone usage policy and procedure.
- Must reimburse the State for any telephone calls, including applicable federal and state taxes that, notwithstanding the provisions of this procedure, are made for personal use.

Agencies:

- Must ensure that employees understand and comply with this policy and procedure. Agencies may require an employee certification for this purpose. Such certification may be obtained in a separate process or, where possible, combined with other similar periodic certifications (e.g., conflict of interest disclosure).
- Review telephone bills for unusual usage and maintain other monitoring processes, as appropriate, to help ensure compliance with this policy and procedure.
- If applicable, maintain employee certifications in personnel files, if certification is required.

\* \* \*

**EXHIBIT A**

**Suggested Format for Employee Certification -  
State Telephone Usage Policy**

Chief Financial Officer \_\_\_\_\_  
Department of \_\_\_\_\_

Dear: \_\_\_\_\_

I, \_\_\_\_\_, understand that usage of the State telephone system or a State issued telephone credit card for other than official State business or as authorized by my employer is prohibited, and all telephone charges are subject to audit, as provided in Section 1210.13 of the *Administrative Guide to State Government*.

In the event that, notwithstanding this policy, I use the telephone system for personal purposes, I will reimburse the State for such telephone charges plus applicable federal and state taxes.

If I misuse the State telephone system for personal purposes, I accept full responsibility for any administrative action taken against me relating to violation of this telephone usage policy.

Sincerely,

_____	_____
Employee Signature	Date
_____	
Division or Office	

IV. DMB PROCEDURE 1310.16  
Issued January 6, 1997

SUBJECT: Acceptable Use of the State Telecommunication Network

APPLICATION: Executive agencies and other non-executive branch entities which use the State data communication networks.

PURPOSE: Provide procedures implementing the acceptable use of the State Telecommunications Network Policy and for all other resources connected to that inter-network.

CONTACT AGENCY: Department of Management and Budget (DMB) - Office of Information Technology Solutions (OITS), Standards and Planning Services Division

TELEPHONE: 517/373-2654

FAX: 517/335-1575

PROCEDURES:

State Network Users Responsibilities:

- Make a reasonable effort to inform themselves of and comply with the acceptable use policies of each system and external network they intend to access, prior to their attempting access.
- Respect the privacy and ownership privileges of other users. Unless authorized to do so, users shall not intentionally seek information on, obtain copies of, use, modify, or place on openly accessible information servers - files and other data which are exempt or excluded from public disclosure pursuant to the Freedom of Information Act (FOIA), PA 442 of 1976, as amended. Release, distribution and handling of FOIA documents and data must conform with Administrative Procedure 2410.01, issued January 1, 1994 and applicable department procedures regarding denial of FOIA requests and other state and federal laws.
- Respect the legal protection provided by copyright and license to programs and data. No software copy is to be made by any user without a prior, good faith determination that such copying is, in fact, permissible and that the licensing restrictions have been met.

- Respect the integrity of passwords and/or authentication pass phrases by complying with state security policy. The exchanging of passwords or seeking the password of others is explicitly prohibited.
- Respect the integrity of computing systems by not intentionally taking actions or developing programs that either harass other users or obstruct a computer system. Users shall not damage, alter, or disrupt computers or maliciously use computer systems whose usage is protected by law, regulation, or administrative policy.
- Respect the integrity of connected computer systems by insuring that imported files are virus free.
- Not represent themselves electronically as others, either on state networks, or elsewhere, unless explicitly authorized to do so by those other users. Users must not circumvent established, system-specific policies defining eligibility for resource access.
- Be good network citizens by being cognizant of and conservative in the bandwidth demands their applications (especially those using video or image transmissions) make on the network. Future bandwidth contention may necessitate restrictions.

#### Acceptable Uses of the Telecommunication Network:

- Communication and exchange directly relating to the mission, charter and work tasks of the state agency.
- Announcements of new state laws, procedures, policies, services or activities, but not commercial advertising
- Use for advisory, standards, research, analysis and professional society activities related to the user's state governmental duties.
- Use in applying for or administering grants or contracts for state government research or programs, but not for non-state government related fund raising or public relations activities.
- Communication and exchange for professional development, to maintain currency, or debate issues related to that user's assigned state governmental activities.

#### Prohibited Uses of the Telecommunication Network:

- Use which is illegal.

- Use which violates the security, privacy and confidentiality policies, practices and laws of the state and release of material which is exempt from disclosure as listed in section 13 of the Freedom of Information Act (Public Act 442 of 1976 as amended).
- Use for access to, display of or distribution of: (a) indecent or obscene material (re US Supreme Court Miller v California 1973 and Ginsberg v New York 1968), (b) child pornography (re 18 US Code 2252) or (c) material in violation of Civil Service Rule 1-2.2 or departmental regulations prohibiting sexual harassment.
- Use for profit activities unless specific to the charter, mission and duties of the government agency.
- Use for private or personal business transactions, or for partisan or non-partisan political activities.
- Use for playing of games or non-business computer activities which generate traffic or consume bandwidth on any state network segment.

AGENCY:

- Agency Chief Information Officers or their delegated representatives are responsible for compliance with provisions of this procedure and for investigating suspected non-compliance. These duties include
  - Investigation of alleged or suspected non-compliance with the provisions of this policy. These are to be conducted with due regard for the privacy rights of all persons and users involved.
  - Suspension of service to users when deemed necessary for the operation and/or integrity of the state communication infrastructure or connected networks. Use privileges, user accounts and/or password access may be withdrawn without notice.
  - When an instance of non-compliance is suspected or discovered in a computing system or network connected to the state network, the agency shall proceed in accordance with departmental and Civil Service rules. Internal discipline, up to and including discharge, may be appropriate in some cases of non-compliance with this policy. Criminal or Civil action may be initiated in appropriate instances.

DMB OFFICE OF INFORMATION TECHNOLOGY RESPONSIBILITIES:

- Maintain this procedure to be in conformance with relevant administrative directives, Michigan Laws and advances in technology.
- Disseminate changes in procedure to all departments and agencies as needed, but no less than annually.

\* \* \*

V. DMB PROCEDURE 1410.15  
Issued January 1, 1994

SUBJECT: Cellular telephones and services.

APPLICATION: Executive Branch Departments and Sub-Units.

PURPOSE: To provide for acquiring cellular telephones and using cellular telephone services, and necessary reimbursement procedures for official use of personal cellular telephones.

CONTACT AGENCY: Department of Management and Budget (DMB) - Telecommunications.

TELEPHONE: 517/373-0785

FAX: 517/373/0303

SUMMARY: To procure or use cellular telephones or cellular telephone services, an agency must identify the need and submit appropriate documentation to the Telecommunications Division.

Reimbursement to employees for official use of personal cellular telephone services must be approved by the respective department director designee.

APPLICABLE FORMS: Telecommunications Requirements Analysis Document for Cellular Telephones and/or Service.

PROCEDURES:

Agency:

- Develops a cellular telephone acquisition and services plan.
- Uses the following criteria to develop justification for specific uses:
  - Only the most essential uses should be authorized for continuation (emergencies, protection of state assets, safety and welfare of citizens or personnel, and communication with the Governor's office.)

Telecom:

- Reviews and approves department plans.
- Reviews and approves specific requests for equipment.

\* \* \*

**ATTACHMENT B**

**DEQ**  
MICHIGAN DEPARTMENT OF ENVIRONMENTAL QUALITY  
OFFICE OF HUMAN RESOURCES

**TELECOMMUNICATION DEVICE ACCEPTABLE USE AGREEMENT**

See DEQ Policy and Procedure 02-001 for instructions regarding processing of this form

EMPLOYEE NAME (Last, First, Middle Initial) <i>(please print or type)</i>	EMPLOYEE SOCIAL SECURITY NUMBER
---	---------------------------------

As a user of Michigan Department of Environmental Quality (DEQ) telecommunication devices, I agree and acknowledge that I:

1. Will comply with the State of Michigan Computer Crime Law (Public Act 53 of 1979);
2. Will use the Michigan Department of Environmental Quality computer systems (as defined in Public Act 53 of 1979) to perform my job functions to the exclusion of all other purposes;
3. Will comply with Civil Service Rules 5-5 (Patents/Inventions) and 5-6 (Copyrights) for any DEQ computer software I develop or participate in development of;
4. Will comply with DMB Procedures 1210.13, 1310.16 and 1410.15 regarding appropriate use of telecommunication devices;
5. Will comply with DEQ Policy and Procedure 02-001 regarding appropriate use of telecommunication devices, including but not limited to, computers, modems, telephones, cellular telephones, voice mail, two-way radios and telefaxes;
6. Have received copies of Public Act 53 of 1979, Civil Service Rules 5-5 and 5-6, DMB Procedures 1210.13, 1310.16 and 1410.15 and DEQ Policy and Procedure 02-001. I understand the information contained in these documents and how it applies to my job. In the event that, notwithstanding any of the statutes, policies or procedures mentioned here, I use any telecommunication device for personal purposes, I will reimburse the State for any telephone or other charges incurred, plus applicable federal and state taxes. Further, I understand that any violation of these laws, rules or procedures may result in disciplinary action or recommendation for prosecution, as appropriate.

EMPLOYEE SIGNATURE	DATE
--------------------	------