

Sample Policies for Internet Use, Email and Computer Screensavers

In many of its financial management reviews, the Technical Assistance Section has encouraged municipalities to develop and adopt policies that address employee use of the Internet and email. Less frequently mentioned is the importance of protecting data and information on computers through screensavers with password security.

In a city, the mayor issues policies for the executive branch of government. In a town, the board of selectmen is the chief policy making body. There will be instances when other municipal boards or individuals will originate a draft or recommend a permanent policy, but final adoption typically requires the approval of the mayor or selectmen.

A standard format for all local policies should be developed. As a rule, a section should be devoted to specifying who the policy applies to. Then, the rules should be enumerated. Expectations relative to employee behavior should be clear. Actions that are regarded as violations should be listed as well as penalties for non-compliance. The policy should also describe an appeal process for an employee, who is found to violate the policy.

By way of example, included below are two policies adopted and implemented by the State Department of Revenue:

“Electronic Messaging and Internet Acceptable Use Policy”
“Screensaver Standard”

MASSACHUSETTS DEPARTMENT OF REVENUE

Electronic Messaging and Internet Acceptable Use Policy

Effective September 16, 2008

Introduction

The Massachusetts Department of Revenue (DOR) encourages responsible, effective and lawful use of the Internet and electronic mail (E-mail) as a means for employees to fulfill their individual job duties and responsibilities. Inappropriate use of your Internet and E-mail privileges can result in disciplinary action up to and including termination of your employment with DOR.

Purpose

In view of the potentially serious consequences that may result from the misuse of the Internet and E-mail at work, DOR has issued this policy to provide you with direction and guidance for the acceptable and responsible use of the Internet and E-mail systems.

Scope

This policy applies to all employees. "Employees" for the purpose of this policy shall include: all full or part-time employees of DOR or its vendors: contract employees; individual consultants; temporary employees; seasonal employees; volunteers; trainees; student interns; members; directors; officers; partners; agents; and subcontractors. The use of DOR resources implies an understanding of an agreement to this policy.

Policy

Employees should have **no expectation of privacy** when using the Internet and Exchange/Outlook, the E-mail messaging system. All Internet and E-mail use is continuously monitored to ensure compliance with this policy. The use of DOR resources constitutes express consent for DOR to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access.

Employees should not use state provided E-mail messaging systems for confidential matters that are not intended for public disclosure. All DOR E-mail users are strongly encouraged to use, *Secure Mail Gateway*, DOR's authorized encrypted secure E-mail option when sending messages outside of DOR.

DOR provided Internet and E-mail messaging systems are state property. Internet and E-mail content residing on DOR networks and computer systems and Internet/E-mail content sent to or from DOR networks and computer systems is DOR property.

Incidental personal use of DOR Internet and E-mail systems, while not encouraged, is permissible at the discretion of divisional management. Personal use must not interfere with an employee's work performance and must not violate the unauthorized use guidelines within this policy.

Internet and E-mail access is a privilege provided to employees to help them conduct official DOR business and may be revoked at any time.

Employees are prohibited from accessing Internet sites or sending any E-mail containing material that is sexually explicit, gambling related or that contains defamatory, harassing, threatening or otherwise offensive content.

Any employee that is requested by an external vendor/consultant/contractor to participate in a remote control type session with the external vendor/consultant/contractor must contact ISO's User Support line at 617-887-5911 or x79511 to request the ability to participate. Each request will be reviewed on an individual basis and a determination issued upon review by ISO.

Employees must not send, forward, receive or store confidential or sensitive DOR information utilizing non-DOR approved mobile devices. Mobile devices include, but are not limited to, Blackberries, Personal Data Assistants (PDA), two-way pagers, cellular telephones or laptops.

Employees must not use the Internet or E-mail to conduct any personal business activity, such as personal banking, purchasing or selling transactions or solicit for religious, charitable or other causes.

Confidential, federal or personally identifiable information must never be transmitted via E-mail unless it is sent utilizing DOR's authorized encrypted secure E-mail option *Secure Mail Gateway*, which is a messenger gateway that allows secure transmission of confidential information through E-mail.

E-mail, including e-mail sent utilizing the *Secure Mail Gateway*, must not contain confidential information in the subject line.

Faxes received in an employee's E-mail inbox may not be forwarded to non DOR E-mail addresses unless they are sent via the secure E-mail option.

Non-business related E-mail sent into DOR via the Internet may be "blocked" and not delivered to the intended recipient. DOR may "block" and prevent employee access to any Internet site.

Employees utilizing DOR issued devices may only access the Internet through DOR approved firewalls. Under no circumstances may employees use modem, WLAN (Wireless Local Area Network), WWAN (Wireless Wide Area Network), connections to access the Internet, thereby, bypassing DOR's Internet infrastructure. The only exception to this prohibition would be to utilize the Internet for remote access purposes to gain access to DOR's VPN (Virtual Private Network) environment.

All Internet pages and E-mail content are scanned for viruses and malicious software and any Internet content containing a virus or malicious software will not be allowed into the DOR network.

DOR's Global Address List will not be made available for public access.

As with any other application, DOR employees are forbidden from sharing their accounts with anyone including but not limited to supervisors, administrators, colleagues, consultants, seasonal staff, etc.

Employees are required to notify the Inspectional Services Division upon receipt of any E-mail containing sexually explicit material and/or content that is defamatory, harassing, threatening or offensive in nature.

Employee Responsibilities

Employees must comply with this policy and all standards, guidelines and laws referenced within this policy.

Employees must safeguard the confidentiality and integrity of DOR information as part of the ongoing business process and their individual work assignments.

Employees are expected to ensure that Internet and E-mail content is appropriate for the workplace and must be able to withstand public scrutiny, as any information contained within E-mail messages or Internet accesses can be subject to public disclosure.

Non-compliance/Unauthorized Use

Unauthorized use of Internet and E-mail includes, but is not limited to:

- Accessing personal or non-DOR mail servers, including personal E-mail accounts, unless granted prior authorization by ISD and ISO.
- Storing or forwarding DOR information using non-DOR mail servers, including personal E-mail accounts, unless granted prior authorization by ISD and ISO.
- Sending obscene, defamatory, harassing or threatening messages or messages containing sexually explicit material.
- Sending or posting any material or images that may be offensive or demeaning to any person based upon their race, sex, religion or sexual orientation.
- Using an unauthorized encryption method or sending unencrypted confidential information, including but not limited to, names, addresses, social security numbers, tax and child support data over the Internet or via E-mail.
- Sending or posting messages with a disguised or false identity.
- Gaining or attempting to gain unauthorized access to any computer, computer records, data, databases or electronically stored information.
- Distributing chain letters, conducting illegal activities, or soliciting information for personal gain or profit via the Internet and/or E-mail is strictly prohibited.
- Engaging in public instant messaging and/or accessing bandwidth intensive services (such as RealAudio or Video or MP3).

- Violating any local, state or federal law.
- Making or posting indecent remarks and proposals.
- Uploading or downloading non-DOR authorized software. Prior to uploading or downloading any software employees must contact ISO's User Support line at 617-887-5911 or x75911 for authorization. Depending on the software download request, ISO may require a formal request defining the business need. This request must come from a supervisor and may be reviewed by ISO as well as ISD.
- Knowingly spreading a computer virus.

Penalties

Non-compliance or unauthorized use of the Internet and/or E-mail may result in the unauthorized disclosure of DOR information, which is a direct violation of federal and state statutes.

Under Massachusetts law:

The unauthorized disclosure of tax return information is punishable by a fine of up to \$1,000 and/or imprisonment for not more than six months and by disqualification from holding office in the Commonwealth for a period not exceeding three years. (M.G.L. c. 62C §21).

- The unauthorized disclosure of wage reporting information is punishable by a fine of \$100 per offense and by administrative discipline. (M.G.L. c. 62E §8).
- The unauthorized disclosure of child support information is punishable by a fine of up to \$1,000 per offense and/or by imprisonment of up to one year and disqualification from holding office in the Commonwealth for a period not exceeding three years. (M.G.L. c. 119A §5A).
- The unauthorized disclosure of personal information, including any information regarding health insurance is prohibited and may result in damage claims from affected individuals. (M.G.L. c. 66A).
- DOR is required to notify any individual, as well as the Attorney General and the Director of Consumer Affairs, Information Technology Division (ITD) and Supervisor of Public Records when the individual's personal information has been accessed or used without authorization. (M.G.L. c. 93H).

Under federal law:

The unauthorized disclosure of federal tax return information and is a felony that may be punished by a fine of up to \$5,000 and/or imprisonment for not more than five years. (26 USC 7213).

Taxpayers have the right to file a lawsuit against you personally for the unauthorized browsing or disclosure of their federal information. (26 USC 7431).

MASSACHUSETTS DEPARTMENT OF REVENUE**Screensaver Standard**
*Effective December 3, 2008***Introduction**

Department of Revenue (DOR) employees must understand the importance of protecting sensitive and confidential data from unauthorized access or acquisition. The information systems used by all DOR employees to carryout day-to-day responsibilities contain very sensitive, confidential information. Employees with direct access to information systems that maintain confidential information such as tax and child support information, as well as those employees that do not have direct access to confidential information, must understand that an unauthorized access to any computer could result in a serious breach of the entire DOR information systems structure.

Purpose

In an effort to ensure the confidentiality and integrity of DOR information, the Department requires all DOR computers to use a timed screen saver with password security enabled.

Scope

This standard applies to all employees. "Employees" for the purpose of this policy shall include: all full or part-time employees of DOR or its vendors: contract employees; individual consultants; temporary employees; seasonal employees; volunteers; trainees; student interns; members; directors; officers; partners; agents; and subcontractors. The use of DOR resources implies an understanding of and agreement to this standard.

Standard

DOR requires screen saver activation after **10 minutes** of user inactivity. Each DOR computer is configured for automatic screen saver activation for the maximum time limit of 10 minutes. Employees are not permitted to manage their own time limit. Requests for exceptions to the 10 minute time limit must be submitted to an employee's respective Deputy Commissioner. Any exception to the 10 minute time limit must be approved by the Senior Deputy Commissioner and will be considered only for legitimate business reasons and for a specified period of time.

Employee Responsibilities

- Employees must comply with this standard and all policies referenced within this standard.
- Employees must activate the screen saver when stepping away or leaving their workstation. The screensaver may be activated by using Ctrl, Alt, & Delete and selecting Lock Workstation or by selecting the Screensaver Shortcut button on the Windows Taskbar.
- Employees must be aware of other individuals in and around your work station when looking at or discussing confidential information.
- Employees must abide by the Department's [Password Policy](#).

Resources and Contact Information

Technical problems with the screen saver functionality should be reported to the ISO Help Desk at 617-887-5911.

Questions regarding the Screensaver Standard should be directed to the Inspectional Services Division at 617-626-2130.

Compliance

Unauthorized use and/or access of DOR computers may result in the unauthorized disclosure of DOR information, which is a direct violation of federal and state statutes.

Under Massachusetts law

The unauthorized disclosure of tax return information is punishable by a fine of up to \$1,000 and/or imprisonment for not more than six months and by disqualification from holding office in the Commonwealth for a period not exceeding three years. (M.G.L. c. 62C §21).

- The unauthorized disclosure of wage reporting information is punishable by a fine of \$100 per offense and by administrative discipline. (M.G.L. c. 62E §8).
- The unauthorized disclosure of child support information is punishable by a fine of up to \$1,000 per offense and/or by imprisonment of up to one year and disqualification from holding office in the Commonwealth for a period not exceeding three years. (M.G.L. c. 119A §5A).
- The unauthorized disclosure of personal information, including any information regarding health insurance is prohibited and may result in damage claims from affected individuals. (M.G.L. c. 66A).
- DOR is required to notify any individual, as well as the Attorney General and the Director of Consumer Affairs, Information Technology Division (ITD) and Supervisor of Public Records when the individual's personal information has been accessed or used without authorization. (M.G.L. c. 93H).

Under federal law

The unauthorized disclosure of federal tax return information is a felony that may be punished by a fine of up to \$5,000 and/or imprisonment for not more than five years. (26 USC 7213).

Taxpayers have the right to file lawsuits against you personally for unauthorized browsing or disclosure of their federal tax information. (26 USC 7431).