THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF LABOR AND WORKFORCE DEVELOPMENT

MASSHIRE

Information Technology Resources Policy

Effective: July 1998, Revised: January 2018

This document formalizes the policy for employees of the Executive Office of Labor and Workforce Development, contractors and other authorized users (hereafter "users") on the use of information technology resources ("Agency ITRs"), including computers, printers and other peripherals, programs, data, local and area-wide networks, the Internet email, facsimile machines, photocopiers, pagers, telephone and cellular phones, voicemail and two-way radios. Use of Agency ITRs by any users shall constitute acceptance of the terms of this policy and any such additional policies.

1. User responsibilities

It is the responsibility of any user of Agency ITRs to read, understand, and follow this policy. In addition, users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of Agency ITRs. Any user with questions regarding the application or meaning of this policy should seek clarification from appropriate management.

The Agency reserves the right to recoup any costs incurred for unauthorized use of ITR. Failure to observe this policy may subject users to disciplinary action, including termination of employment.

2. Acceptable uses

The Executive Office of Labor and Workforce Development firmly believe that Agency ITRs empower users and make their jobs more fulfilling by allowing them to deliver better services at lower costs. As such, users are encouraged to use Agency ITRs to the fullest extent in pursuit of the Agency's goals and objectives.

3. Unacceptable uses of Agency ITRs

It is unacceptable for any user to use Agency ITRs:

- in furtherance of any illegal act, including violation of any criminal or civil laws or regulations,
- whether state or federal;
- for any political purpose;
- for any commercial purpose;
- to send threatening or harassing messages, whether sexual or otherwise;
- to access or share sexually explicit, obscene, or otherwise inappropriate materials;
- to infringe any intellectual property rights;
- to gain, or attempt to gain, unauthorized access to any computer or network;
- for any use that causes interference with or disruption of network users and resources,
- including propagation of computer viruses or other harmful programs;
- to intercept communications intended for other persons;
- to misrepresent either the Agency or a person's role at the Agency;
- to distribute chain letters;
- to access on-line gambling sites; or
- to libel or otherwise defame any person.

4. Data confidentiality

In the course of performing their jobs, users may often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for users to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may users disseminate any confidential information, unless such dissemination is required by their jobs.

5. Copyright protection

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a website. As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgment when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

6. Computer viruses

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any questionable source. In addition, executable files (program files that end in ".exe") should not be stored on or run from network drives. Finally, it is a good practice to scan floppy disks periodically to see if they have been infected.

7. Network security

Most desktop computers are connected to a local area network, which links computers within the Agency and, through the wide area network, to most other computers in state government. As such, it is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users should never share their passwords with anyone else, and should promptly notify the EOLWD Information Security Office (part of the EOLWD Internal Control & Security Department) if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should either log off the network or have a password protected screensaver in operation. Finally, no user is allowed to access the Internet or other external networks via modem unless they have received specific permission from EOLWD Information Security Office.

8. Email

When using email, there are several points users should consider. First, because email addresses identify the organization that sent the message (user@detma.org), users should consider email messages to be the equivalent of letters sent on official letterhead. For the same reason, users should ensure that all emails are written in a professional and courteous tone. Finally, although many users regard email as being like a telephone in offering a quick, informal way to communicate, users should remember that emails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an email message that they would not feel just as comfortable putting into a memorandum.

9. No expectation of privacy

Agency ITRs are the property of the Commonwealth of Massachusetts and are to be used in conformance with this policy. The Agency retains, when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer. Users should be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic. Use of Agency ITRs constitutes express consent for the Agency to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any websites that they access. The Agency does not intend to monitor the content of telephone conversations without prior notice. However, the usage of telephone communication is monitored for the performance of agency operations, maintenance, auditing, security, or investigative functions.

10. Remote access

Some users will be authorized by the Agency for remote access to email and other applications. Access is authorized for the same purposes as other Agency resources, i.e., business use. Managers should approve remote access only for those users which have a job-related need to access Agency resources remotely. Users authorized for remote access to email and other applications are required to read, sign

and comply with the terms and conditions explained in the Remote Access User Certification Agreement, which is Attachment B to this policy.

All users of the Agency's Information Technology Resources are required to read and comply with this policy. Additionally, all users are required to sign (along with the responsible Executive Office of Labor and Workforce Development manager) and submit Attachment A to this policy, the ITR Policy Acknowledgement Form.

Users requesting remote access are required to read, comply, sign (along with the responsible Executive Office of Labor and Workforce Development manager) and submit the Remote Access User Certification Agreement, which is Attachment B to this policy.

All users of the Agency's Information Technology Resources are required to read and comply with this policy and to acknowledge that they have received and read the policy by signing off on the Policy Acknowledgement Form provided to them each year.

Attachment "A"
Information Technology Resources Policy

Acknowledgment form for employees and non-employees

Section 1: to be completed by employee or non-employee

I hereby acknowledge receipt of the Policy concerning the use of Executive Office of Labor and Workforce Development (EOLWD) Information Technology Resources (ITR). I understand that as:

Check one: ☐ an employee ☐ a non-employee

using ITR resources of the Commonwealth, it is my responsibility to read and comply with the requirements of this Policy.

_____ _____
Print name Organization/Company (Non-Employees)

_____ _____
Signature Date

Section 2: to be completed by Manager responsible for employee or non-employee

As the EOLWD Manager responsible for the above named individual, I understand that it is my responsibility to monitor the above named individual's compliance with the ITR Policy and to notify the Office of Internal Control and Security (ICS) of any violations. I also understand that I must notify ICS when the above named individual's services conclude so that his/her access is promptly terminated.

_____
Print name

_____ _____
Signature Date

Please return completed original acknowledgement form to:

Executive Office of Labor and Workforce Development
Office of Internal Control and Security
100 Cambridge Street
Boston, MA 02114

Attachment "B"
Information Technology Resources Policy

Remote Access User Certification Agreement

Section 1: to be completed bv employee or non-employee

I hereby acknowledge receipt of the Policy concerning the use of Executive Office of Labor and Workforce Development (EOLWD) Information Technology Resources (ITR). Further, I understand that as:

Check one: ☐ an employee ☐ a non-employee

working for or with EOLWD, otherwise referred to as "the Agency," I am being granted the privilege of Remote Access because management has determined that I have a job-related need for remote access to Agency ITR. I also understand that it is my responsibility to read the provisions of this Agreement and comply with its requirements. By engaging in remote access of ITR, I will adhere to the following provisions:

1. Use Remote Access only for official Commonwealth business.

2. Comply with the terms and conditions of the Agency Confidentiality Agreement and agree not to store any confidential information on any system used to gain Remote Access.

3. Not access or disseminate confidential data unless such access or dissemination is required by my job. The user is responsible for ensuring that his or her Remote Access use of the ITR systems does not inappropriately expose the data in the remote environment or compromise security of the systems or applications.

4. Protect and not share with anyone my password or the Universal Resource Locator (URL) provided to me for Remote Access. Should a user have reason to believe that his or her password has been compromised, the user must immediately report this event to the Office of Internal Control and Security (ICS) to ensure that the password can be reset or the code can be revoked or inactivated.

5. Acknowledge that the user is responsible for maintaining all end user remote access systems that are the property of the user, which includes handling technical problems, providing the hardware, software and Internet provider connections necessary for remote access, and ensuring that antivirus software is installed, running and updated regularly.

6. Have no expectation of privacy in the use of Information Technology Resources.

7. Allow the Agency to monitor and/or inspect any data that the user sends or receives, any information that the user sends or receives, and any sites with which the user may exchange information.

8. Allow the Agency to exercise the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer when reasonable and in pursuit of legitimate agency needs.

Terms and conditions of work

This agreement to and acknowledgement of the Remote Access provision of the ITR policy does not modify any existing term and/or condition of employment between the employee and the employer, including the hours of work. Overtime must be authorized in advance by the appropriate manager or supervisor.

Violations of Policy

Violations of the policies and provisions specified above may result in termination of access to Information Technology Resources, including Remote Access, and may also result, where applicable in disciplinary action up to and including termination of employment.

Print name	Organization/Company (Non-Employees)
Title	Phone
Signature	Date

Section 2: to be completed by Manager responsible for employee or non-employee

I certify that I am the EOLWD manager of the above named individual and that Remote Access is needed by this individual for official Commonwealth business only. I understand that it is my responsibility 1) to review Remote Access accounts annually to ensure that there is a continuing need for the remote access resources and privileges; and 2) to monitor the above named individual's compliance with the ITR policy and 3) to notify ICS at (617) 626-6680 of any violations. I also understand that I must notify ICS when the above named individual's services conclude so that his or her access is promptly terminated.

Print name	Office location
Title	Phone
Signature	Date

Please return completed original agreement to:

Executive Office of Labor and Workforce Development
Office of Internal Control and Security
100 Cambridge Street
Boston, MA 02114