THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF LABOR AND WORKFORCE DEVELOPMENT

REMOTE ACCESS ACCEPTABLE USE POLICY

Effective: July 2014

1. Purpose

The Executive Office of Labor and Workforce Development (EOLWD) is comprised of the Department of Career Services (DCS), Department of Industrial Accidents (DIA), Department of Labor Standards (DLS), Department of Labor Relations (DLR) and the Department of Unemployment Assistance (DUA). EOLWD and its Departments are committed to managing the confidentiality, integrity, and availability of their information technology networks, systems, and applications. This includes establishing guidelines for remote access (by use of Citrix or VPN for example) to the organization's critical information assets maintained within the IT Systems. Remote access is the process of accessing EOLWD Electronic Information Resources from networks that are not controlled by EOLWD. This policy defines the appropriate security measures that are required for the user to remotely connect to EOLWD networks.

The purpose of this policy is to define standards for connecting to the EOLWD network from any host. These standards are designed to minimize the potential exposure to EOLWD from damages that may result from unauthorized use of EOLWD resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical EOLWD internal systems, and damage to the public's confidence in our agency.

2. User Responsibilities

It is the responsibility of any EOLWD Electronic Information Resources user to read, understand, and follow this policy. In addition, all users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of EOLWD Electronic Information Resources. Any user with questions regarding the application or meaning of this policy should seek clarification from appropriate management. EOLWD reserves the right to recoup any costs incurred for unauthorized use of EOLWD Electronic Information Resources.

3. Enforcement

Failure to observe and adhere to this policy may subject users to disciplinary action, up to and including immediate revocation of remote access privileges, termination of employment (if applicable), as well as possible civil and criminal penalties.

4. Scope

This policy applies to all individuals who are granted remote access privileges to EOLWD Electronic Information Resources. Those individuals covered include, but are not limited to employees, partners, staff, contractors, consultants, those working on behalf of the agency, and/or individuals authorized by affiliated institutions and organizations. This policy applies to remote access connections used to do

work on behalf of EOLWD, including but not limited to, connecting to EOLWD resources, reading or sending e-mail and viewing intranet web resources.

All remote access implementations at EOLWD are covered by this policy including dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, Citrix Access Gateway, Outlook Web Access, and hardware or services provided by third parties.

Anyone who accesses, uses, or controls EOLWD Electronic Information Resources via remote methods is subject to, and must adhere to, this policy.

5. No Expectation of Privacy

5.1 Agency Owned Devices

All EOLWD IT resources are the property of the Commonwealth of Massachusetts and are to be used in conformance with this policy. EOLWD retains the right to inspect any user's agency-owned device using agency remote access methodologies, 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 IT resources constitutes express consent for EOLWD to monitor and/or inspect any data that users create or receive, any messages they send or receive, any files created or maintained and any web sites that they access.

5.2 Non-Agency Owned Devices

All devices not owned by EOLWD and used for Commonwealth business must be used in compliance with all Commonwealth laws and Agency policies. EOLWD retains the right to inspect any data sent into the agency network or extracted from the agency network. This includes but is not limited to personally owned smart phones, tablets, laptops, or desktop computers that have been used in the creation, storage or transmitting of Agency data. Users should be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic. Use of agency IT resources constitutes express consent for EOLWD to monitor and/or inspect any agency-related data that users create or receive and any messages they send or receive.

6. Policy

Prior to accessing the EOLWD network remotely (via Citrix, or VPN) the following multi-layer security strategy must be implemented by all users to defend against malicious attacks and unauthorized access that can compromise your device. A Remote User's device must be at least as secure as its on-site counterpart.

6.1 General

A. Users must ensure proper physical security precautions are taken when connecting to the EOLWD network from remote locations. For example:

a. Screen saver policies and/or other safeguards must be followed if a machine must be left unattended while connected or logged into the EOLWD network;

b. In public environments, users should take precautions to prevent unwanted viewing of their device's screen by unauthorized persons. Sensitive (confidential or secret) EOLWD information must not be read, discussed, or otherwise exposed in restaurants, on

airplanes, on trains, or in other public places where unauthorized people might discover it.

c. Public computers or devices (such as public library PC's or kiosks) should never be used to access EOLWD systems

d. Citrix should only be used in designated/approved locations.

B. Anyone granted remote access to EOLWD resources must not remotely access agency systems and/or data from a network outside of the United States boundaries, and must not take confidential agency information into another country unless the permission has first been obtained from EOLWD management and Internal Control and Security (ICS).

C. Remote Access privileges may include the ability to download or print documents/files that contain confidential business information. Any documents/files downloaded or printed via Remote Access shall be managed in accordance with agency practices for retention and destruction of confidential information (documents containing confidential information shall be cross-cut shredded before disposal, or carried back to a EOLWD location and deposited in a locked recycle bin).

D. When connecting to the EOLWD network with wireless connections on personal networks, the wireless connections must be encrypted using WEP or other acceptable secure technology. If connecting through a router that has a wireless transmitter, whether connected through either the wired or wireless ports, the transmitter must be configured in an encrypted mode or it must be turned off.

E. Users of remote access privileges shall not transfer confidential or sensitive data from a secure site to an unsecured device or location (e.g. a notebook or home personal computer) unless absolutely necessary. If confidential or sensitive data is transferred to a laptop, refer to the Laptop Policy for data handling requirements.

F. The Agency will engage in ongoing annual remote access security reviews to verify the identities of current remote access users and their continuing need for such access. Greater frequency of such reviews may be required based on the sensitivity or confidentiality required by the data being accessed.

G. Portable computing devices (laptops, tablets, smartphones, etc) and portable electronic storage media that contain confidential, personal, or sensitive EOLWD information must use encryption or equally strong measures to protect the data while it is being stored. Portable electronic storage media includes, but is not limited to USB or Flash Drives, CDs, Removable hard drives.

6.2 Agency Owned Devices

A. Remote users must comply with federal, state, and local law and all EOLWD policies.

B. All Remote User activity during a remote session is subject to EOLWD policies and may be monitored and logged for compliance.

C. Secure remote access must be strictly controlled. Access to EOLWD IT Resources will be controlled through the EOLWD-authorized remote access method (e.g. Citrix Access Gateway or VPN) utilizing a user ID and password.

D. Remote Users must ensure that their EOLWD-owned computer or device, which is remotely connected to the EOLWD network, is not connected to any other network at the same time other than a Private Network under the user's control

6.3 Non-Agency Owned Devices

A. Implement credible and reputable anti-virus software (e.g., Symantec or McAfee Antivirus), perform continuous and/or scheduled scanning, and keep it up-to-date. An anti-virus program will protect your computer from malicious programs. The software must be operating at all time in real time scan mode, the virus definition list shall be updated at least once a day, and schedule a weekly full system scan.

B. Implement anti-spyware to protect your private information. Spyware is a class of programs designed to steal personal information. The software must be operating at all times and the definition list shall be maintained up-to-date.

C. Enable the built-in firewall that is included in major operating systems (i.e., Windows and Macs). A firewall is an application to restrict others from connecting to your computer. The firewall application should be set to restrict access unless required by specific applications.

D. Check for vendor security updates and apply them (e.g. Windows, Adobe, Flash). Periodically, security weaknesses in the operating system and/or application are discovered and the vendor will then provide security updates to remediate such security exposures. Enable the automated feature in major operating systems (i.e., Windows and Macs) that checks for security updates. When notified of the security updates availability, review the updates and then apply updates as appropriate.

E. Establish strong password syntax (i.e. - at least 8 alphabet & numeric characters, refer to EOLWD Password Policy) and protect your password. A password is used to provide authentication to an application and/or system. Never share your password with anyone even family members.

F. Limit your computer usage to yourself and restrict others from using it, especially for internet access because they may unintentionally download malicious software (e.g., key logging program) for which you will be accountable.

G. Remote users must comply with federal, state, and local law and all EOLWD policies.

H. All Remote User activity during a remote session is subject to EOLWD and all relevant laws (State and Federal).

I. Secure remote access must be strictly controlled. Access to EOLWD IT Resources will be controlled through the EOLWD-authorized remote access method (e.g. Citrix Access Gateway or VPN) utilizing a user ID and password.

J. Remote Users must ensure that their non-EOLWD-owned personal or business device, which is remotely connected to the EOLWD network, is not connected to any other network at the same time other than a Private Network under the user's control. In cases where the remote user is accessing EOLWD resources from their non-EOLWD place of work, secure network practices and procedures must be in use by the company or organization’s IT department.

K. If remote access privileges are granted to a user for use from the home computer, the user is responsible for all costs incurred in acquiring hardware, software (except for the remote access client software), and internet connections necessary for remote access.

7. General

Users must use the EOLWD supplied remote access method (e.g. Citrix client software or VPN certificate) for remote desktop access to the EOLWD network.

Contact the EOLWD IT Help Desk for more information and assistance on remote desktop access.

The EOLWD IT Help Desk must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

All remote access users (via Citrix or VPN) are required to read and comply with this policy. Additionally, all users are required to sign (along with the responsible EOLWD manager) and submit the Remote Access Acknowledgment and User Certification Agreement.

Inquiries: Please email all questions to ICID@detma.org.

REMOTE ACCESS USE POLICY

REMOTE ACCESS ACKNOWLEDGMENT AND USER CERTIFICATION AGREEMENT

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

I hereby acknowledge receipt of the Remote Access Use Policy. I understand that as:

Check One: ☐ an employee ☐ a non-employee

working for or with EOLWD, otherwise referred to as "the Agency", that Remote Access is a privilege granted to me because management has determined that I have a job-related need for remote access to Agency Information Technology Resources (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 use, I will adhere to the following provisions:

1. Remote access use is exclusively 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 to 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. 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 & Security (ICS) to ensure that their password can be reset or their 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 the handling of technical problems, providing the hardware, software and Internet provider connections necessary for remote access, and that anti-virus software is installed, running and updated regularly.

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

7. For agency owned devices, 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. For agency and non-agency owned devices, Allow the agency to exercise the right to inspect any user's computer or device, any data contained in it, and any data sent or received by that device when reasonable and in pursuit of legitimate agency needs. Agency or non-agency devices include, but are

not limited to, smart phones, tablets, laptops, or desktop computers that have been used in the creation, storage or transmitting of Agency data.

Terms and Conditions of Work

This agreement to and acknowledgement of the Remote Access policy does not modify any existing policy, term and/or condition of employment between the employee and the employer including the hours of work.

Violations of Policy

Failure to observe and adhere to this policy shall subject users to disciplinary action, up to and including immediate revocation of remote access (Citrix or VPN) privileges, termination of employment (if applicable), as well as possible civil and criminal penalties.

_____	_____
PRINT NAME	ORGANIZATION / COMPANY (non-employees)
_____	_____
TITLE	TELEPHONE
_____	_____
SIGNATURE	DATE

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

I certify that I am the manager of the above named individual and that remote access use is needed by this individual for official Commonwealth business only. I understand that it is my responsibility to: 1) review remote access use accounts annually to ensure that there is a continuing need for remote access use by this individual; and 2) to monitor the above named individual's compliance with this 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	TELEPHONE
_____	_____
SIGNATURE	DATE

Please return completed original Certification Agreement to:
Executive Office of Labor & Workforce Development
Office of Internal Control & Security
19 Staniford Street, 4th Floor
Boston, MA 02114