MASSACHUSETTS WORKFORCE DEVELOPMENT SYSTEM

MassWorkforce Issuance

Workforce Issuance No. 06-07 ☑ **Policy** ☐ **Information**

To: Chief Elected Officials
Workforce Investment Board Chairs
Workforce Investment Board Directors
Title I Administrators
Career Center Directors
Title I Fiscal Officers
DCS Associate Directors
DCS Field Managers

cc: WIA State Partners

From: Susan V. Lawler, Director
Division of Career Services

Date: February 10, 2006

Subject: **Network Security Protocols**

Purpose: To notify all Local Workforce Investment Boards, One-Stop Career Center Operators, IT Administrators, Workforce Partners, staff, and other concerned parties about network security protocols for all equipment connected to the detma.org network.

Background: The Department of Workforce Development is under Federal Information Security Management Act (FISMA) audit findings to improve network security and reduce the likelihood of the compromise of, or complete loss of sensitive federal, business and personal data. As a result, beginning in December 2005 the DWD Information Technology Department has been extending the use of existing core network security protocols from the central network to the local office and Career Center level.

NOTE: These network security protocols produce the consequence that the unauthorized addition of, or movement of computing equipment attached to the network *will result in the immediate and automatic shutdown of the device in question*.

Policy: To avoid loss of connectivity to the network (including connection to MOSES and to Exchange email) take the following steps:

- If you are planning to move equipment that is connected to the network, contact the DWD IT Department Help Desk prior to the move at 617-626-5555. They will ensure that the IT Department works with you to make sure that all network security protocols are addressed prior to your planned move.

- If you are replacing or adding equipment to the network, contact the DWD IT Department Help Desk prior to installing the new equipment at 617-626-5555. They will ensure that the IT Department works with you to authenticate all new equipment properly on the network to guarantee that network security protocols are not breeched.

- If you are considering switching off a piece of equipment on a temporary basis (e.g., disconnecting a CPU to hook up a laptop to the network), contact the DWD IT Department Help Desk prior to installing the new piece of equipment at 617-626-5555. They will ensure that the DWD IT Department works with you to make sure that all network security protocols are addressed so that the equipment works properly and so that the original equipment can be restored after the temporary use of the connection.

- If you accidentally caused a network connection to shut down at your location, you will need to contact the DWD IT Department Help Desk at 617-626-5555. You will need to provide them with your name, your specific location, the time of lost connectivity, and the cause of the security breech in order for them to re-enable network access for the computer or device in question.

This directive applies to any and all devices connected directly to the Detma.org network including computer CPUs, network printers, and network-attached multi-function machines (all-in-one copier/scanner/fax/printers). Laptop computers also are covered by this directive if you intend to plug them into an existing port on the network (e.g., to conduct a Quality Assurance review or data validation).

Action Required: Please assure that all appropriate staff are informed of the content of this issuance.

Inquiries: Please direct inquiries about this issuance to PolicyQA@detma.org . If you encounter a problem with devices on the detma.org network, please contact the DWD IT Department Help Desk at 617-626-5555.