MASSHIRE | DEPARTMENT OF CAREER SERVICES

Workforce Issuance

100 DCS 03.109 ☑ **Policy** ☐ **Information**

To: Chief Elected Officials
MassHire Workforce Board Chairs
MassHire Workforce Board Directors
Title I Administrators
MassHire Career Center Directors
Title I Fiscal Officers
MDCS Operations Managers

cc: WIOA State Partners

From: Alice Sweeney, Director
MassHire Department of Career Services

Date: January 31, 2019

Subject: **Massachusetts Identity Theft Legislation**

Purpose: To provide policy guidance to MassHire Workforce Boards, MassHire Career Center Operators and other local workforce partners with respect to state legislated requirements for securing customers' personal information in order to prevent identity theft. *Note: this policy replaces MassWorkforce Issuance No. 07-81 and has been updated with current nomenclature; the content is unchanged.*

Background: The Commonwealth enacted legislation regarding Identity Theft Prevention which requires everyone who handles 'personal information' (defined below) to ensure that this information is safeguarded at all times. Under the legislation, "personal information" is defined as an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

a. Social Security number;

b. driver's license number or state-issued identification card number; or
c. financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account.

Policy: To ensure compliance with the requirements of the Commonwealth's Identity Theft legislation, MassHire Workforce Boards and MassHire Career Center Operators must review local policies and procedures to assure consistency with the following precautionary practices and requirements:

1. **Files, documents, reports and media (e.g. disks/flash drives) containing personal information** should never be unattended/unsecured during the workday and must be properly secured at the end of each workday. This should be done by securing the items containing personal information in offices, rooms, desk drawers and file cabinets that can be locked.

2. **Boxes of files ready to be stored and awaiting pickup**: If, while awaiting permanent storage, there is a need to temporarily store boxes of files that may contain personal information within offices or general space within the Board or career center, it is critically important to secure these boxes of files while they await pickup.

3. **Files containing personal information that are/need to be located on any network shared drive**, whether it is the MassHire Department of Career Services (MDCS) "X" drive or another shared drive should only be accessible by those staff members who need to utilize the information as part of their job duties.

4. **Electronic transmission:** personal information should never be transmitted electronically to persons or entities outside of MDCS and/or local network unless sufficient safeguards have been taken (i.e. encryption, secure socket) prior to transmission.

Breach of Security Requirements

M.G.L. Chapter 93 was amended by the Identity Theft legislation to cover requirements regarding breaches of security and unauthorized access and use of personal information. Should a breach of security occur or there is reason to believe that a breach has occurred with respect to the personal information of a resident of the Commonwealth or when it is known or reasonably believed that the personal information has been acquired or used by an unauthorized person or used for an unauthorized purpose, M.G.L. Chapter 93H requires notification to certain parties.

To whom or to what entity notice is to be given depends on the "ownership" status of the personal data that has been or is suspected to have been breached

or accessed/used in an unauthorized manner. The legislation differentiates between a "legal" person (a "natural person, corporation, association, partnership or other legal entity) and an agency (any agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or of any political subdivision thereof").

As a MassHire Workforce Board is not an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, MassHire Workforce Boards are considered to fall under the definition of "legal" person. Unless a MassHire Career Center is a direct unit of a local government it also is considered to fall under the designation of "legal" person.

M.G.L. Chapter 93H Section 3(a) requires a "legal" person or agency that *maintains and stores, but does not own or license* personal information about a resident of Massachusetts to provide notice only to notify the "owner or licenser" of the personal data. In such cases, the person or entity *is not required* to notify the individual whose personal information was or may have been breached or accessed/used in an unauthorized manner.

M.G.L. Chapter 93H, Section 3(b) requires a "legal" person or agency that "owns or licenses" the personal information of a resident to notify the resident of the actual or suspected breach or the actual/suspected unauthorized access/use of the personal data.

Additionally, Chapter 93H, Section 3(b) also requires the owner or licenser of the personal data to provide formal notice to the Massachusetts Office of the Attorney General and to the Massachusetts Office of Consumer Affairs *and* Business Regulation.

In all cases, whether notification is generated in accordance with Chapter 93H §3(a) or 93H §3 (b), the notice must include, but is not limited to:

- the date or approximate date of said incident,
- the nature of the actual or suspected breach, and
- any steps taken or planned relating to the incident

In all cases, notice must be given "as soon as practicable, and without unreasonable delay" of the actual or suspected breach or unauthorized access/use.

For incidents covered by the Identity Theft legislation with respect to personal data of MassHire Career Center customers *owned* by MDCS (MOSES data, UI Claims Data, etc.) Career Center operators must assure that all managers and staff *immediately* report the incident (or suspected incident) to the EOWLD

Internal Control and Security Office at 617-626-6680 or ICID@MassMail.State.MA.US.

For incidents covered by the Identity Theft legislation with respect to personal data of MassHire Career Center customers *owned* by the career center or the MassHire Workforce Board and *not owned* by MDCS, the Board and/or Career Center operator must adhere to the notification requirements described above.

Action Required: Please ensure that all MassHire Workforce Board staff and MassHire Career Center management and personnel are informed of and knowledgeable of the contents of this issuance.

Effective: Immediately

Inquiries: Please email all questions to PolicyQA@MassMail.State.MA.US; indicate Issuance number and description.