STATE OF MARYLAND
DLLR
DEPARTMENT OF LABOR, LICENSING AND REGULATION

# POLICY ISSUANCE 2019-04

**Privacy and Data Security | March 28, 2019**

**TO:** Division of Workforce Development and Adult Learning (DWDAL) staff;
Local Workforce Development Area directors;
Local Administrators of WIOA Title II Adult Education provider programs

**FROM:** Division of Workforce Development and Adult Learning
Maryland Department of Labor, Licensing and Regulation

**SUBJECT:** Privacy and Data Security

**PURPOSE:** To provide comprehensive policy guidance on protection and use of Personally Identifiable Information (PII) and sensitive information and the obligations to DWDAL regarding any breach.

**ACTION:** WIOA Title I Local Workforce Development Area Directors, WIOA Title II local grant administrators, American Job Center (AJC) Labor Exchange Administrators, and central office managers will ensure all employees are aware of and receive copies of this policy. DWDAL policies are available on the DLLR website. WIOA Title I Local Workforce Development Area Directors and WIOA Title II local grant administrators will develop privacy and data security policies.

**EXPIRATION:** Until cancelled or replaced.

## QUESTIONS:


Lauren Gilwee, Director
Policy
DLLR DWDAL
410.767.2268
lauren.gilwee@maryland.gov

Lloyd Day, Director
Office of Workforce Development
DLLR DWDAL
410.767.2995
lloyd.day@maryland.gov

Alice Wirth, Director
Office of Correctional Education
DLLR DWDAL
410.767.9769
alice.wirth@maryland.gov

Terry Gilleland, Director
Office of Adult Education & Literacy Services
DLLR DWDAL
410.767.1008
terry.gilleland@maryland.gov

Carolyn Mitchell, Director
Office of Workforce Information and Performance
DLLR DWDAL
410.767.2953
carolyn.mitchell@maryland.gov

Tanya Washington, Manager
Office of Monitoring and Compliance
DLLR DWDAL
410.767.2098
tanya.washington@maryland.gov

Chris MacLarion, Director
Apprenticeship and Training
DLLR DWDAL
410.767.3969
christopher.maclarion@maryland.gov

Michael DiGiacomo, Executive Director
DLLR Governor's Workforce Development Board
410.767.2131
michael.digiacomo@maryland.gov

*****

# TABLE OF CONTENTS

## PRIVACY AND DATA PROTECTION

# GENERAL INFORMATION

## WORKFORCE INNOVATION & OPPORTUNITY ACT

The Workforce Innovation and Opportunity Act (WIOA) was signed into law on July 22, 2014, and went into effect July 1, 2015. WIOA supersedes the Workforce Investment Act of 1998 (WIA) and amends the Adult Education and Family Literacy Act, the Wagner Peyser Act, and the Rehabilitation Act of 1973. By design, the workforce system established under WIOA is integrated to help both businesses and jobseekers. WIOA envisions connecting businesses with job seekers, through meaningful partnerships among workforce, education, human services, and economic development entities to ensure optimum results and leveraging of resources. The law addresses the needs of job seekers through establishing a workforce system that helps them access employment, education, training, and support services to succeed in the labor market. Through the American Job Centers (AJCs), WIOA works to address employer needs by matching them to the skilled workers they need to compete in the global economy.

In order to ensure that AJCs and WIOA programs are effectively serving both jobseekers and employers as well as meeting federal compliance requirements, states must collect participant and program-level data to track performance. Local and state partners are bound by law to protect customer and employee sensitive information and Personally Identifiable Information (PII), both in electronic and physical file format.

## SENSITIVE AND PERSONALLY IDENTIFIABLE INFORMATION

Sensitive information includes any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled under various state and federal laws. PII is participant-level and employee data that either by itself or combined with other data can link to a specific individual or identity. PII is divided into two categories: protected and non-sensitive. Protected PII falls under the sensitive information category. While non-sensitive PII has a much lower risk of harm if misused, confidentiality must still be maintained.

Protecting PII and sensitive information is a federal and state priority. The differences between protected PII and non-sensitive PII are laid out in **Table 1: Examples of Protected and Non-Sensitive PII** below.[1] The examples of protected PII and non-sensitive PII are not meant to be an exhaustive list of PII elements.

**Table 1: Examples of Protected and Non-Sensitive PII**

| Type of Data | Definition | Examples |
|---|---|---|
| Protected PII | Information that, if disclosed, could result in harm to the individual whose name or identity is linked to that information. | Examples of protected PII include, but are not limited to, social security numbers, credit card numbers, driver's license numbers, bank account numbers, telephone numbers,[2] ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords. |
| Non-Sensitive PII | Information that if disclosed, by | Examples of non-sensitive PII include information |

[1] Training and Employment Guidance Letter (TEGL) 39-11, "Guidance on the Handling and Protection of Personally Identifiable Information (PII)," dated June 28, 2012.

[2] MD. Code Ann. Gen. Prov.§4-101(f) (vii) defines "telephone number" as personal information. COMAR 09.01.04.13A(3) includes "personal phone number" as sociological information.

| | | |
|---|---|---|
| | itself, could not reasonably be expected to result in personal harm. It is stand-alone information that is not linked or closely associated with any protected or unprotected PII. | such as first and last names, email addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII. |

## FEDERAL ACTS ON PRIVACY AND DATA SECURITY

At the federal level, a number of laws[3] exist to ensure customer data protection, including:

- The Privacy Act of 1974,
- The Family Educational Rights and Privacy Act (FERPA),
- The Health Insurance Portability and Accountability Act (HIPAA), and
- The Social Security Act.

### The Privacy Act of 1974

The Privacy Act of 1974 governs the collection, maintenance, use, and dissemination of PII maintained in systems of records by federal agencies. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the individual, unless the disclosure is permissible under one of twelve statutory exceptions. The Privacy Act also provides individuals with a way to seek access to an amendment of their records and establishes various agency record-keeping requirements.

### The Family Educational Rights and Privacy Act (FERPA)

FERPA protects PII contained in a student's educational record, applying to both the K-12 system and postsecondary institutions.

### The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Title II protects the privacy and confidentiality of medical records and patient PII in any media form. HIPAA's provisions on privacy and breach[4] notification extend to plans, clearinghouses, and all other health record keeping entities that use electronic data transfer systems.

### The Social Security Act

The Act defines the administration of the state's Unemployment Insurance program, and its corresponding regulations define and protect the confidentiality of unemployment records.

[3] This list is not meant to be exhaustive but instead is recognition of the laws most likely to affect participants in workforce programs. The applicability of a particular law or regulation may be different for the partners based on various legal and factual scenarios.
[4] See pages 13-17 for more information on security breaches.

## MARYLAND'S APPROACH TO DATA SECURITY

Maryland follows federal requirements as well as state law to protect PII and sensitive information. The Maryland Personal Information Protection Act (PIPA)[5] was passed in 2008 and amended in 2018. PIPA mandates that businesses protect customers', employees', and former employees' PII and notify them in the case of a security breach of electronic records. Maryland also requires the protection of information by Government Agencies.[6] Both statutes contain notification requirements under certain circumstances.

Maryland is committed to increasing the earning capacity of Marylanders, which will support businesses. This goal can only be achieved through working in partnership in the WIOA system, including the Department of Labor, Licensing and Regulation (DLLR); Department of Human Services; Division of Rehabilitation Services, Department of Housing and Community Development, Governor's Workforce Development Board, and the Maryland Workforce Association. Each partner has its own data and data system(s), thus each has the need to protect customer and employee privacy. This policy is meant to provide guidance for the protection of DLLR's Division of Workforce Development and Adult Learning (DWDAL)-specific data, as well as in handling partner data attained through Data Sharing Memoranda of Understanding (MOUs).[7] It is the policy of DWDAL to protect all information about an individual (including jobseekers, program participants, businesses, and employees) maintained by the agency, including protected PII, non-sensitive PII, and sensitive information.

Maryland recognizes that the best course of action is to avoid a security breach; however, in the case that a security breach does occur, the state expects that vendors and local and state staff follow the procedures as laid out in this policy to address and rectify the breach. Local entities, including Local Areas, WIOA Title II local grant administrators, and vendors, operating under DWDAL oversight or with access to DWDAL data must have a data protection policy or directives in place, including incident response plans in the case of loss of data. As part of the incident response plan, entities should identify an incident response team in advance.

This policy should not be construed as including all of a partner's responsibilities if a security breach occurs. There are numerous legal requirements under state and federal law which must also be followed. Additionally, partners may be subject to requirements in a data sharing agreement.

### Division of Workforce Development and Adult Learning's Collection and Use of Data

DWDAL administers a number of WIOA state Plan programs, including the Title I Adult, Dislocated Worker, and Youth programs; Title II Adult Education and Family Literacy Act program; Title III Wagner-Peyser Act program; Correctional Education program; Trade Adjustment Assistance for Workers program; Jobs for Veterans State Grant program; the Senior Community Service Employment Program; Registered Apprenticeship; and more. For these programs, DWDAL and local partners collect participant-level demographic data at initial eligibility determination and during the delivery of basic and individualized career services, training, and follow-up services. Data collection helps the programs to:

- Determine eligibility for participation in WIOA programs;
- Determine eligibility for inclusion on Maryland's Eligible Training Provider List[8];
- Determine barriers to employment and provide supportive services, where applicable;

[5] Md. Code Ann. Comm. Law §§14-3501 *et seq.*
[6] Md. Code Ann. State Gov't §10-1301 *et seq.*
[7] See page 8 for more information on Data Sharing Memoranda of Understanding (MOUs).
[8] For more information on Maryland's Eligible Training Provider List, see DLLR Policy Issuances, available at: http://www.dllr.state.md.us/employment/mpi/

- Track and ensure that programs (including state and local partners) are helping customers as they are intended to do;
- Track performance metrics;
- Track co-enrollment of customers;
- Track follow-up with customers;
- Highlight whether the programs are serving diverse populations and individuals with barriers to employment (e.g. data elements self-identified disability and Limited English Proficiency status);
- Help Maryland understand the state of the workforce system; and
- Assist Maryland in applying for and attaining federal grants.

## DWDAL Data Systems

DWDAL warehouses data in two main data systems, the Maryland Workforce Exchange (MWE) and the Literacy, Adult and Community Education System (LACES).

The MWE serves as the data system for a number of WIOA programs, including the WIOA Title I Adult, Dislocated Worker, and Youth programs; WIOA Title III Wagner-Peyser Employment Services, Jobs for Veterans State Grant Program, and the Trade Adjustment Assistance for Workers Program. The MWE is used for reporting as well as labor market information needs for its job candidates, workforce professionals, and employers. Currently, PII and sensitive information are stored and protected through the MWE, where partners can only see information that is pertinent to their work. Additionally, limited read-only confidential Unemployment Insurance (UI) information can be viewed through the MWE system and must be protected accordingly. MWE is a secure platform to protect the confidentiality of customers. DWDAL staff and WIOA Title I Local Areas have access to and submit data to the MWE. Department of Human Services staff will have access to a MWE module for Supplemental Nutrition Assistance Program.

LACES serves as the data system for WIOA Title II Adult Education and Family Literacy Services as well as Correctional Education. LACES does not have a public-facing function and is used for internal data management. LACES data is not stored in the MWE.[9] DWDAL staff and WIOA Title II adult education grantees have access to and submit data to LACES.

While the MWE and LACES are the division's two main data systems, smaller systems also exist. For instance, the Maryland Apprenticeship and Training Program uses the Apprenticeship Information Management System (AIMS) and the Registered Apprenticeship Partners Information management Data System (RAPIDS). DWDAL staff have access to and submit data to AIMS and RAPIDS. Additionally, the Correctional Education program, while housed in LACES, is also linked to and subject to rules and regulations of the Department of Public Safety and Correctional Services.[10] Any new functionality or systems incorporated into the system are covered by this policy.

[9] Temporary Assistance for Needy Families, Vocational Rehabilitation, Community Service Block Grant, and Re-Integration of Ex-Offenders also do not house data within the MWE. Each of these programs is overseen by a different agency or organization, each with their own data system.

[10] This policy is not meant to be exhaustive as to how data must be handled in an individual correctional facility; rather, this policy is an overview of data protection measures that must be taken for physical and electronic data, including for future data systems the division may procure.

# ACCESS TO DATA SYSTEMS

A limited number of local and state staff have access to DWDAL data systems to track customers, labor market information, co-enrollment, etc. Additionally, state partners can gain read-only access to DWDAL data through a Data Sharing MOU, listing the specific pieces of data they can access as well as their purposes for viewing that data.[11]

## CUSTOMER RELEASE OF INFORMATION

The Maryland Workforce Exchange includes a customer disclaimer, which allows for the sharing of performance data between DWDAL and approved partner agencies.[12] This disclaimer does not eliminate the need for a customer Release of Information.

Prior to sharing customer PII or sensitive information, the customer must sign a Release of Information to acknowledge that certain records will be shared with the relevant partner entity. The customer Release of Information must be maintained in the customer's physical or electronic file with the customer's authentic signature. The Release of Information must specify which records the customer is consenting to share, the entity that the information will be shared with, and the customer's signature. Local entities may use their own form for customer release.

In the event that there are more specific requirements in a data sharing agreement, the entity must follow the more specific requirements.

## DATA SHARING MEMORANDA OF UNDERSTANDING

It is important to note that the DLLR DWDAL and the DLLR Division of Unemployment Insurance have a Data Sharing MOU in place that gives DWDAL access to certain Unemployment Insurance (UI) wage record information. For local partners to receive access to the MWE system, including the confidential UI wage data within MWE, the applicable Local Workforce Development Area (Local Area) must have a MOU in place with DLLR, meeting the confidentiality requirements of federal and state law for UI information. DWDAL will only grant MWE read-only access to partners in Local Areas that have requisite MOUs in place with DLLR.[13]

## STAFF ROLES & RESPONSIBILITIES

To maintain customer and employee data protection, all staff and partners with access to participant-level data must:

- Complete the Staff Confidentiality Agreement every six months and submit it to the director of the appropriate DWDAL office granting the access, according to the chart below. The attachments in **Table 2: Staff Confidentiality Agreement by Data System** provide sample agreements that staff must complete and submit.

[11] For more information on read-only access to the MWE, see DLLR Policy Issuances, available at: http://www.dllr.state.md.us/employment/mpi/

[12] A list of the partner agencies covered by the Maryland Workforce Exchange disclaimer can be found at the following link: https://mwejobs.maryland.gov/vosnet/security.aspx?a=disclaimer

[13] This is not an all-inclusive list of MOUs in place between DLLR and its partners. This policy covers all current and future Data Sharing MOUs with DLLR.

**Table 2: Staff Confidentiality Agreement by Data System**

| Data System | Agreements are Submitted to | Attachment |
|---|---|---|
| MWE[14] | Director, Office of Workforce Development | ***Attachment A – Staff Confidentiality Agreement: Maryland Workforce Exchange*** |
| LACES | Director, Office of Adult Education & Literacy | ***Attachment B – Staff Confidentiality Agreement: Adult Education and Literacy Services*** |
| Correctional Education Student Database | Director, Office of Correctional Education | ***Attachment C – Staff Confidentiality Agreement: Correctional Education*** |
| RAPIDS or AIMS | Director, Apprenticeship and Training | ***Attachment D – Staff Confidentiality Agreement: Apprenticeship*** |

- Maintain client confidentiality and protect PII, sensitive information, confidential UI data, and educational records[15];
- Inform DLLR of any users who were previously granted access to a DLLR data system and need to be restricted or inactivated within ten business days of decision to inactivate user;
- Participate in training for the protection of PII and sensitive information on-hire and on an annual basis; and
- Notify mandated and relevant parties in the case of a security breach, as outlined on pages 13-15, and as required by other legal or contractual requirements.

## Data Training Responsibilities

Any vendor, local, or state staff with access to electronic or physical participant-level data must undergo training on the handling and protection of data as well as protocol in case of a breach (1) upon hire and (2) annually afterwards. DLLR will provide core training on protection of PII and sensitive information. Local entities are responsible for more in-depth training specific to their local policies, incident response plan, flow of physical files, and electronic data systems. Training may be conducted online and/or combined with other ethics training (e.g. ethics with handling Unemployment Insurance data).

[14] Individuals with access to the MWE system that are not employed by the DLLR central office should follow DLLR DWDAL policy issuance "Partner Access to the Maryland Workforce Exchange (MWE)" in submitting their Staff Confidentiality Agreements. DLLR DWDAL current and archived policy issuances are available online at: http://www.dllr.state.md.us/employment/mpi/.

[15] See pages 10-12 for information on protection of PII and sensitive information.

# PROTECTION OF DATA AND SENSITIVE INFORMATION

Both physical and electronic formats of PII and sensitive data must be protected. Any staff, manager, etc. with access to participant-level data must ensure confidentiality and protection of customer and employee information. In order to protect PII and sensitive data, individuals with authorized access should be aware of which data is sensitive and/or protected, as described in **Table 1: Examples of Protected and Non-Sensitive PII** on pages 4-5 of this policy. While neither physical nor electronic, staff must also maintain verbal protection[16] of customers' confidential information. Staff may not verbally share customers' PII or sensitive data with others that do not have approved access to that data.

The following sections provide guidance on how to protect physical and electronic data.

## PHYSICAL DATA SECURITY REQUIREMENTS

Physical data refers to paper files, as required for record retention, auditing, and often used in case management. Safeguards to protect physical data must include:

- Reducing the volume of collected and retained physical data to the minimum necessary as is needed for reporting, eligibility determination, and case management;
- Limiting access to those individuals who must have access to perform job functions;
- Keeping files in cabinets and offices that lock;
- Keeping equal opportunity data (e.g. medical information and requests for accommodations) in files separate from employees' personnel files in accordance with 29 CFR Part 38.41;
- Ensuring that all cabinets and offices are locked before leaving the office unattended;
- Ensuring that files are not left out (e.g. on a desk during a lunch break) where an unauthorized individual can access them;
- Developing and adopting a risk-aware culture;
- Conducting due diligence on all third-party service providers and requiring appropriate information security standards to be written into contracts;
- Conducting on-hire and annual training on the protection of physical data;
- Developing a data governance policy and/or procedures;
- Developing and testing an incident response plan, which should involve key stakeholders;[17]
- Using unique identifiers to de-identify records and remove PII (e.g. new unique number specific to organization versus use of social security number);
- Using locked boxes when transferring data for auditing; and
- Using confidential recycling to dispose of records.

Additionally, DWDAL strongly recommends the following best practices in safeguarding electronic data:

- Limiting the number of records removed from secure storage to only those immediately in use and
- Using a paper file tracking log.

[16] When interacting with clients, staff must take reasonable steps to ensure privacy when PII must be shared verbally.
[17] Incident response plans should cover the loss of records, e.g. from a natural disaster.

## Retention and Disposal of Physical Records

Local and state partners must maintain participant-level data for specific timeframes according to the type of record, including three years for workforce program data, seven years for fiscal data, and five years for adult education data, or until all audit and litigation issues are resolved, whichever is later. If any litigation, claim, or audit is started before the expiration of the standard retention period, the records then must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action has been taken. DLLR must maintain Registered Apprenticeship data in accordance with the Department for General Services' Records Retention and Disposal Schedule. Once the mandated amount of time has passed for a physical record, and the record is not needed as follow-up to an audit finding or concern, then the record may be disposed of. Disposal must take the form of confidential recycling, such as with a cross-cut shredder or through a vendor.

# ELECTRONIC DATA SECURITY REQUIREMENTS

Electronic data refers to participant-level data retained in electronic data systems, such as the MWE or LACES. These data banks contain large sources of data that are necessary for state and program function but are also potential vulnerable targets for breaches. Safeguards to protect electronic data must include:

- Reducing the volume of collected and retained electronic data to the minimum necessary;
- Limiting data access to only those individuals who must have such access;
- Using password-protection, encryption-preferred[18], strong authentication procedures, and other security controls to make the information unusable by unauthorized individuals (necessary when transmitting PII through email or other electronic format; e.g. staff may not email social security numbers without encryption, even if the email is addressed to an individual that has authorized access[19]);
- Immediately deleting received emails containing unencrypted PII and instructing the sender to also delete (including removing from the "deleted files" folder) the email from their "sent" and "deleted files" folders;
- Ensuring that data is not left unattended (e.g. MWE data must not be left open on screen while on a lunch break);
- Logging out of data systems when leaving one's desk;
- Limiting network access to approved devices certified with appropriate security controls;
- Not accessing data systems from non-secure computers (e.g. personal computer);
- Conducting due diligence on all third-party service providers and requiring appropriate information security standards to be written into contracts;
- Following all electronic and physical record requirements when scanning a document into a data system, including not using PII or sensitive information in the naming convention of scanned documents;
- Conducting on-hire and annual training on the protection of electronic data;
- Developing a data governance policy and/or procedures;
- Developing and testing an incident response plan, which should involve key stakeholders; and
- When receiving data requests:
    - Providing aggregate-level data (i.e. all PII and sensitive information removed and performance numbers combined to represent the whole program or class) or

[18] Encryption refers to the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.

[19] When it is necessary to send PII through email, staff must ensure that the recipient is the only person who has access to the information and that the recipient understands they also must protect the information. Participant information must only be communicated through agency approved email addresses and not through third party or personal email addresses.

- If participant-level is required, only providing participant-level data if the entity or partner has an MOU in place.

Additionally, DWDAL strongly recommends the following best practices in safeguarding electronic data:

- Setting computers to go to screensaver after a maximum of five minutes of inactivity;
- Setting computer to lock after a maximum of 15 minutes of inactivity;
- Developing and maintaining access by documenting and reviewing users and roles regularly;
- Blocking PII and sensitive information from being downloaded to individual devices (e.g. flash drive);
- Developing and maintaining an inventory of all hardware and software;
- Using the most current versions of applications and operating systems;
- Requiring complex passwords and using multi-factor authentication;
- Developing and adopting a risk-aware culture;
- Conducting vulnerability testing and risk assessments;
- Investing in cyber insurance;
- Using unique identifiers to de-identify records and remove PII (e.g. new unique number specific to organization versus use of social security number); and
- Implementing access control for mobile devices.

## Retention and Disposal of Electronic Records

Participant-level data must be maintained for specific timeframes according to type of record. The retention periods of electronic files should match the physical file schedules for corresponding records.[20] After the retention period has passed, electronic records should be cleared, purged, or destroyed, such that the PII and sensitive information cannot be retrieved. The receipt of electronic records from other entities may be subject to additional requirements defined by specific data sharing agreements.

[20] If DWDAL procures different data systems in the future, the existing data should be migrated over to the new system, as applicable to the retention period.

# SECURITY BREACHES

The term "breach" is used to indicate the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.[21] Breaches can be the result of a spontaneous incident (e.g. data system error), security incident (e.g. break-in), privacy incident (e.g. failure to maintain confidentiality), staff error, data breach, etc. Breaches are hazardous both to customers and to organizations involved. Individual harm may include identity theft, embarrassment, or blackmail. Organizational harm may include a loss of public trust or legal liability. ***Attachment E – Job Aid: Security Breach*** provides a summary flow chart of the steps that staff need to take in the event of a security breach.

Upon discovery of a security breach, organizations are required to notify affected parties and oversight agencies, assess the level of potential harm as a result of the breach, develop a Corrective Action Plan, and activate the incident response plan. Organizations are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

## RECOGNIZING A SECURITY BREACH HAS OCCURED

Security breaches vary by cause, magnitude, and effect. Thus, there are multiple ways to recognize that a security breach has occurred. If a staff member or partner suspects that a security breach has occurred, they must notify their supervisor immediately in order to investigate whether there has been an incident. Examples of warning signs that a security breach has occurred include:

- Missing files or documents,
- Signs of a break-in or attempted break-in to office or cabinets,
- Critical electronic file change,
- Unusually slow internet or devices,
- Obvious device tampering,
- Locked user accounts,
- Unusual electronic outbound traffic,
- Abnormal administrative user activity,
- Fake antivirus messages,
- Redirected internet browsing, and/or
- Unexpected software installs.

## NOTIFICATION TO DWDAL

Breaches are subject to notification requirements, both for physical and electronic data. Upon suspicion that a breach has occurred, the individual that discovered the possible breach must immediately notify their

[21] Office of Management and Budget, Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007.

supervisor. The table below outlines which entities need to be notified[22] at a minimum, by type of program, in the event of a breach:

**Table 3: Notification Parties in the Event of a Breach**

| Workforce Program | Adult Basic and Literacy Education Program | Correctional Education Program | DLLR Central Office and Governor's Workforce Development Board |
|---|---|---|---|
| • For WIOA Title I, Local Area Director (or designee);<br>• For WIOA Title III, Labor Exchange Administrator;<br>• DLLR DWDAL Director of Workforce Development;<br>• DLLR DWDAL Manger of Monitoring and Compliance;<br>• DLLR DWDAL Director of Office of Workforce Information and Performance, where applicable; and<br>• Affected customers/employees; and<br>• Governor's Workforce Development Board Executive Director. | • DLLR DWDAL Director of Office Adult Education and Literacy Services,<br>• DLLR DWDAL Manger of Monitoring and Compliance,<br>• Grantee programs, and<br>• Affected customers/employees. | • DLLR DWDAL Director of Office of Correctional Education,<br>• DLLR DWDAL Manger of Monitoring and Compliance, and<br>• Affected customers/employees. | • DLLR DWDAL Manger of Monitoring and Compliance;<br>• DLLR DWDAL Director of Office of Workforce Information and Performance, where applicable; and<br>• DLLR DWDAL Assistant Secretary;<br>• DLLR Secretary;<br>• Affected customers/employees; and<br>• Governor's Workforce Development Board Executive Director. |

Whether the breach occurred within local, state, or vendor records, the breached entity must notify the organizations and individuals, as outlined in **Table 3: Notification Parties in the Event of a Breach** within three business days. For each breach, the DLLR DWDAL Monitoring and Compliance Manager must be notified as soon as possible. Entities must not wait to notify DLLR until after an investigation has been conducted, for timing is essential to resolving breach issues and protecting customers and employees. The DLLR DWDAL Monitoring and Compliance Manager, then, is in charge of notifying appropriate state and federal partners of the breach within 24 hours if the breach is assessed to have a high level of harm (high impact breach). The DLLR DWDAL Director of the Office of Workforce Information and Performance must be notified of any electronic breach that involves the MWE.

The notifications should be brief and contain the following elements:

[22] Additional notifications may be required based on state and federal laws as well as entities' data sharing agreements. This chart is not meant to define all the responsibilities an entity may have as a result of a breach or suspected breach but is meant to define partner's responsibilities to notify DWDAL.

- A brief description of what happened, including the date(s) and rough time estimate(s) of the breach and of its discovery;
- To the extent possible, a description of the types of PII and/or sensitive information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, disability code, etc.);
- What the agency, organization, or entity is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches;
- Contact information for the organization's person of contact leading the efforts for the investigation; and
- For notifications to the affected customers and/or employees, the steps that affected individuals and/or employees should take to protect themselves from potential harm.

***Attachment F – Sample Initial Incident Report*** provides a template for notifications that need to occur within the organization, the Local Area, and DLLR. The report should be as specific as possible and must be updated if more findings arise.

Organizations experiencing the breach have the responsibility of demonstrating that all required notifications have been provided or that a use of disclosure of unsecured PII or sensitive information did not constitute a security breach. The organization should maintain documentation that all required notifications were made, or alternatively, documentation to demonstrate that notification was not required.

## ASSESS THE LEVEL OF BREACH, RISK, AND HARM

Not all security breaches are the same; the magnitude of possible harm is reliant on a number of factors. For instance, the leak of non-sensitive PII (e.g. gender or race) is not likely to negatively impact the customer. However, a breach of protected PII (e.g. social security numbers) or multiple information points that can be linked together could result in identity theft. As such, in the event of a security breach, any partner that becomes aware of the breach should investigate the following factors to assess the likely risk of harm, including:

- Whether the breach was physical or electronic (where applicable, organizations should immediately shut down all compromised systems to contain an attack or malware infection)[23];
- Nature and sensitivity of the data elements breached;
- Identifiability of data (i.e. the likelihood that an individual can be identified from the data);
- Entity whose data was breached;
- Number of individuals affected;
- Likelihood the information is accessible and usable;
- Likelihood that the breach may lead to inconvenience; and
- Likelihood that the breach may lead to harm.

The entity or organization experiencing the breach must assess these factors; however, other partners are encouraged to additionally assess the factors as they relate to their own clients. A breach within an AJC may affect some or all of the partners (e.g. co-location, co-enrollment, data sharing, etc.).

[23] The initial point of attack may not be the only part of a system that has been compromised. Organizations should check all of their systems and equipment to determine if other areas of the network have also been compromised.

The factors playing into assessing the breach have the possibility to cause either a low, medium, or high level of harm. In a low impact breach, individuals or the organization may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.). In a medium impact breach, individuals or the organization may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.). They may lose capability of finishing or completing an activity as scheduled due to the physical or electronic PII breach (e.g. through identification of family status). In a high impact breach, individuals or the organization may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.) or irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.). Examples of high impact breach include the possibility to cause harm such as blackmail, defamation using person's name in precarious situations, mental or physical harm, loss of benefits, harm to staff assisting clients, number of files or type of data breached.[24]

## CORRECTIVE ACTION PLAN

In response to the notification and incident report, the DWDAL Office of Monitoring and Compliance, in collaboration with the Office of Workforce Development, Office of Adult Education and Literacy Services, the Office of Correctional Education, and/or the Office of Workforce Information and Performance, as is relevant, will issue a letter that outlines concerns and required actions with a deadline. The organization experiencing the breach then must remedy the security breach through a Corrective Action Plan, detailing how they will correct what has happened and next steps. The plan should be designed to rectify the breach and make sure that it does not happen again. Local and/or state staff should use the Corrective Action Plan to analyze how they can better protect their records and maintain customer and employee confidentiality. The Corrective Action Plan should cover all phases of an incident response, including preparation, identification, containment, eradication, recovery, and lessons learned.

There is no single method of responding to a security breach. Each incident must be dealt with on a case-by-case basis by assessing the circumstances and associated risks to inform the appropriate course of action. Corrective Action Plans outline the course of action appropriate for the specific circumstances of an individual incident. Corrective Action Plans must include the following components:

- Completion of the Incident Report;
- Identification and activation of an incident response team (e.g. CIO, Data Coordinator, IT Manager, legal counsel, etc.);
- A timeline indicating which individuals and/or entities were notified of the breach;
- Results of the assessment of level of breach, risk, and harm;
- An analysis of what caused the security breach;
- A determination as to whether the breach was a spontaneous event, security incident, privacy incident, data breach, etc.;
- Identified lessons learned and recommendations for remedial actions that can be taken to reduce the likelihood of recurrence (e.g. review of policies and refresher trainings);
- Identified remedies for impacted customers;

[24] The cases provided in this list of levels of harm are not meant to act as an all-inclusive list; they are examples of the various levels and magnitudes of impact of harm.

- Recovery of lost records, if applicable;
- Measures that the organization will take to prevent such a breach in the future, where applicable; and
- Where applicable, close of the incident case file and reporting.

The Corrective Action Plans create a system for accountability for the implementation of an improved process or rectification of a breach. For each corrective action, the plan should outline who is responsible for each item, what the corrective actions are, and when the corrective actions are completed or projected to be completed. The DWDAL Office of Monitoring and Compliance can then use this plan to follow-up that the security breach has been addressed.

# CONSEQUENCES OF NONCOMPLIANCE AND MONITORING

## CONSEQUENCES OF NONCOMPLIANCE

Local and state partners are bound by law to protect customer and employee PII and sensitive information, both in electronic and physical file format. The failure to do so, or to address a security breach, will result in state, and possibly federal, action. This policy does not address any additional criminal and civil liabilities which may be found in the relevant state and federal laws or as otherwise defined by any specific data sharing agreements entered into by partners but is limited to a partner's duty to DWDAL.

Consequences of failure to address a security breach will be based on the level of harm and magnitude of the breach.

There may be additional penalties, including monetary penalties, criminal penalties, contractual and personal employment consequences, etc.

### Lack of Policy or Directives

Local entities, including Local Areas, WIOA Title II local grant administrators, and vendors, operating under DWDAL oversight or with access to DWDAL data must have a data protection policy or directives in place, including incident response plans in the case of loss of data. For Local Areas, Local Workforce Development Boards must sign off on the policy and/or directives and ensure that staff understand its provisions. The state of Maryland should be able to randomly test to see if a policy and/or directives have been implemented. Local policies should be updated as is appropriate.

### Unauthorized Disclosure of PII and Sensitive Information

DLLR expects local and state staff to maintain customer and employer confidentiality and to protect their PII and sensitive information. The state will take corrective action with any participating organization not meeting the state's expectations for protection of PII and sensitive information and/or unauthorized disclosure of PII.

Corrective action will include technical support and monitoring in the area of concern. If a participating individual fails to correct the unauthorized disclosure, the state may elect to remove that individual's access to data systems or physical files of PII and sensitive information.

### State and Federal Level of Failure to Address Security Breach

If a vendor or local or state staff fail to address a security breach, then DLLR may take the following actions:

- Send a warning letter of noncompliance;
- Removal or restriction of access to PII and sensitive information in physical files and/or data systems;
- Send a letter of noncompliance to alert and mobilize the Governor's Workforce Development Board and the DLLR Secretary's Office for further action;
- Request action before providing funding; and/or
- Reduce funding.

## MONITORING

The state of Maryland acknowledges that the USDOL has the authority to monitor fiscal and/or programmatic protection of PII and sensitive information.

To ensure that policies are being followed and expectations are being met, the state, Local Areas, and all grantees should expect DLLR to conduct monitoring.

Vendors should expect Local Areas to conduct monitoring of vendor contracts as well as fiscal and/or programmatic protection of PII and sensitive information.

# REFERENCES

## LAW

- Workforce Innovation and Opportunity Act (WIOA), 29 U.S.C. § 3101 *et. seq* (2015);
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (1974), as amended;
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended;
- Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 201 (1996), as amended;
- Maryland Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law §§14-3504 (2008), as amended;
- Maryland Public Information Act (MPIA), Md. Code Ann., Gen. Prov. §§ 4-401 *et seq*;
- Md. Code Ann., Lab. & Empl. §8-625 (confidentiality of UI records) as amended;
- Md. Code Ann., Lab. & Empl. § 8-1305 (criminal liability for unauthorized disclosure of UI data) as amended;
- Md. Code, State Gov't Art. §§ 10-1301 *et seq.* (Protection of Information by Government Agencies) as amended;
- Md. Code, Crim. Law § 7-302 (unauthorized access to computers and related material);
- Md. Code, Crim. Law § 8-606 (making false entries or unauthorized access to public record) as amended;
- Md. Code, Correctional Services §3-601 (case records; disciplinary action; property; financial accounts).

## REGULATION

- 29 C.F.R. Part 31, "Implementation of the Nondiscrimination and Equal Opportunity Provisions of the Workforce Innovation and Opportunity Act";
- 34 CFR Part 99, "Family Educational Rights and Privacy";
- 45 CFR Part 5b, "Privacy Act Regulations";
- 21 CFR Part 21, "Protection of Privacy";
- 45 CFR Part 160, "General Administrative Requirements";
- 45 CFR Part 164, "Security and Privacy";
- 20 CFR 603 "Administration of Unemployment Program";
- COMAR 13A.08.02, "Student Records";
- COMAR 07.01.07, "Confidentiality of Records".

## FEDERAL GUIDANCE

- Training and Employment Guidance Letter (TEGL) 39-11, "Guidance on the Handling and Protection of Personally Identifiable Information (PII)," dated June 28, 2012;
- TEGL 26-07, "Job Bank Security Fraud Awareness," dated January 23, 2008;
- TEGL 7-16, "Data Matching to Facilitate WIOA Performance Reporting," dated August 23, 2016;
- TEGL 5-08, "Policy for Collection and Use of Workforce System Participants' Social Security Numbers," dated November 13, 2008.
- Office of Management and Budget Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007.

## OTHER RESOURCES

- National Institute of Standards and Technology, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," dated April 2010;

- European Union Agency for Network and Information Security, "Handbook on Security of Personal Data Processing," dated December 2017.

# ATTACHMENTS

- Attachment A – Staff Confidentiality Agreement: Maryland Workforce Exchange
- Attachment B – Staff Confidentiality Agreement: Adult Education and Literacy Services
- Attachment C – Staff Confidentiality Agreement: Correctional Education
- Attachment D – Staff Confidentiality Agreement: Apprenticeship
- Attachment E – Job Aid: Security Breach
- Attachment F – Sample Initial Incident Report

Attachment A

**Confidentiality Certification**
**For Access to**
**DLLR's Maryland Workforce Exchange Virtual One Stop User Data**

I understand that I will or may be exposed to certain confidential information from records maintained by Maryland Department of Labor, Licensing and Regulation, Division of Workforce Development and Adult Learning (DWDAL) or certain confidential information from records maintained by the Division of Unemployment Insurance ("DUI"), which have been released to my employer pursuant to an Agreement and/or Memorandum of Understanding. Such information, hereinafter referred to as "Confidential Data" may include, but is not limited to: names; addresses; social security numbers; wages; employment data; and other unemployment insurance ("UI") information which is private and confidential and may not be disclosed to others. I have read and understand this Maryland Workforce Exchange (MWE) User and Confidentiality Agreement ("Agreement"). I understand that this Agreement must be renewed annually and that I may be required to complete trainings or additional acknowledgements to retain system access granted by DWDAL and DUI. In exchange for access to the system I acknowledge and agree to abide by the following standards for the receipt and handling of confidential information:

1. I agree to maintain the confidentiality of the Confidential Data including but not limited to information included in the MWE system and safeguard all computer and system passwords, logon identification number and/or names assigned to me for access to the MWE or other government computer systems and/or access to or entry of computer records.

2. I agree to refrain from duplicating Confidential Data for any reason except as specifically authorized by DWDAL and DUI.

3. If I should become aware that any other individual, other than an authorized employee of my employer, may have obtained or has obtained access to my username, password or other information needed to access records maintained by DWDAL or DUI, I shall immediately notify DWDAL and DUI and immediately change my password.

4. I will regard electronic data and other manually maintained records on individual persons, businesses, and/or employers, as confidential in nature, to be held in trust and shall protect such data and systems against unauthorized disclosure and/ or use. These data shall include, but are not limited to, name, address, social security number, tax identification number, age, sex, ethnic background, disability, veteran's status, wage, employment status, education, date of birth, and business information. I will avoid discussing the substance and/or the specific content of the Confidential Data (e.g. sharing log in credentials) or any portion thereof with any other individual or entity. I will refrain from posting or inadvertently causing to be posted images that may disclose Confidential Data information to friends or acquaintances on social networks or any portion of the Internet.

5. I grant DWDAL and DUI the right to inspect, without notice to me, any work created on or information transmitted over the network, including all e-mail messages that are sent or received on the network, accessed internet sites, and information downloaded from or transferred via the internet. By accessing and using DWDAL and DUI information technology resources, I consent to such monitoring and information retrieval for law enforcement and other purposes. I have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media.

6. I will use the system only within the scope of my authorization and within the bounds of the authorization granted by the registered system users. I understand that unauthorized use of or access to information technology resources may result in criminal prosecution and disciplinary action.

7. I shall retain Confidential Data only for that period of time necessary to perform my duties or to comply with the purposes set forth in the Agreement.

8. I have either been trained in the proper use and handling of Confidential Data or I have received written

standards and instructions in the handling of such data. I shall comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which Confidential Data may be kept; and c) following procedures for the timely disposal, destruction or deletion of Confidential Data.

9. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I further acknowledge that applicable state law may provide that any individual who discloses Confidential Data in violation of state law or regulation may be subject to a fine and/or a period of imprisonment and may also result in disciplinary action, up to and including termination. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.

10. Should I have any questions concerning the handling or disclosure of Confidential Data, I shall immediately notify DWDAL and DUI and be guided by advice given by DWDAL and DUI regarding the handling of Confidential Data.

11. I agree the nondisclosure provisions of this Agreement shall survive the termination of this Agreement and that I remain under a duty to hold confidential information in confidence.

I understand that failure to maintain the obligations stated within this agreement may result in loss of access to the data.

Employee Signature: _____ Date: _____

Employee Name (printed): _____

Agency: _____

Address:

_____

_____

_____

Work Telephone: _____

Email: _____

Attachment B

**Authorized Personnel and Agents of Data Requestor**

Data Requestor shall limit access to the Confidential Data to the Authorized Personnel (identified by name, position, and type of access) of Data Requestor listed below for authorized purposes. Data Requestor agrees that only the access necessary for the purposes set forth in this Agreement will be granted. In accordance with DLLR's Division of Workforce Development and Adult Learning Privacy and Data Security Policy, as amended from time to time, Data Requestor will keep this Appendix current and notify Internal Security of additions and/or deletions via email to donata.mooring@maryland.gov.

| Name | Position | Employer | LACES Read-Only Access (check if applicable) | LACES Full Access (check if applicable) | GED Manager Access (check if applicable) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Confidentiality Certification**
**For Access to**
**DLLR's Adult Education and Literacy Services Confidential Data**

I understand that as a result of my employment I will or may be exposed to certain confidential information from records maintained by the Maryland Department of Labor, Licensing and Regulation, Division of Workforce Development and Adult Learning ("DWDAL"). Such information, hereinafter referred to as "Confidential Data," may include, but is not limited to, names, addresses, social security numbers, birth dates, and/or educational records, which is private and confidential and may not be disclosed to others. I understand that this certification must be renewed periodically depending on the access I have been granted or requirements of DWDAL. I acknowledge and agree to abide by the following standards for the receipt and handling of Confidential Data:

A. I shall not disclose my username (if applicable), password (if applicable), or any other information needed to access Confidential Data maintained by DWDAL to any party nor shall I give any other individual access to this information.

B. If I should become aware that any other individual, other than an authorized employee, agent, contractor, or subcontractor of my employer, may have obtained or has obtained access to my username, password or other information needed to access records maintained by DWDAL, I shall immediately notify DWDAL and immediately change my password.

C. I will not share with anyone any other information regarding access to Confidential Data records maintained by DWDAL unless I am specifically authorized by DWDAL.

D. I will not request access to any Confidential Data unless such access is necessary for the performance of my official duties.

E. I will not disclose any Confidential Data to any parties who are not authorized to receive such information (including but not limited to relatives, friends, etc.) except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) involved.

F. I shall retain Confidential Data only for that period of time necessary to perform my duties or to comply with the purposes set forth in the Grant Award. Thereafter, I shall either arrange for the retention of such information consistent with federal record retention requirements or delete or destroy such data.

G. I have either been trained in the proper use and handling of Confidential Data or I have received written standards and instructions in the handling of such data. I shall comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which Confidential Data data may be kept; and c) following procedures for the timely disposal, destruction or deletion of Confidential Data.

H. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I further acknowledge that applicable state law may provide that any individual who discloses Confidential Data in violation of state law or regulation may be subject to a fine and/or a period of imprisonment and dismissal from public service. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.

I. Should I have any questions concerning the handling or disclosure of Confidential Data, I shall immediately notify DWDAL at donata.mooring@maryland.gov and be guided by advice given by DLLR/DUI and/or DWDAL regarding the handling of Confidential Data.

Employee Signature: _____ Date: _____

Employee Name (printed): _____

Employer: _____

Address:

_____

_____

_____

Work Telephone: _____

E-Mail: _____

**Authorized Personnel and Agents of Data Requestor**

Data Requestor shall limit access to the Confidential Data to the Authorized Personnel (identified by name, position, and type of access) of Data Requestor listed below for authorized purposes. Data Requestor agrees that only the access necessary for the purposes set forth in this Agreement will be granted. In accordance with DLLR's Division of Workforce Development and Adult Learning Privacy and Data Security Policy, as amended from time to time, Data Requestor will keep this Appendix current and notify Internal Security of additions and/or deletions via email to danielle.cox@maryland.gov.

| Name | Position | Employer | LACES Read-Only Access (check if applicable) | LACES Full Access (check if applicable) | GED Manager Access (check if applicable) | Correctional Education Student Database Access (check if applicable) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Confidentiality Certification**
**For Access to**
**DLLR's Correctional Education and**
**Adult Education and Literacy Services Confidential Data**

I understand that as a result of my employment I will or may be exposed to certain confidential information from records maintained by the Maryland Department of Labor, Licensing and Regulation, Division of Workforce Development and Adult Learning ("DWDAL"). Such information, hereinafter referred to as "Confidential Data," may include, but is not limited to, names, addresses, social security numbers, birth dates, and/or educational records, which is private and confidential and may not be disclosed to others. I understand that this certification must be renewed periodically depending on the access I have been granted or requirements of DWDAL. I acknowledge and agree to abide by the following standards for the receipt and handling of Confidential Data:

A. I shall not disclose my username (if applicable), password (if applicable), or any other information needed to access Confidential Data maintained by DWDAL to any party nor shall I give any other individual access to this information.

B. If I should become aware that any other individual, other than an authorized employee, agent, contractor, or subcontractor of my employer, may have obtained or has obtained access to my username, password or other information needed to access records maintained by DWDAL, I shall immediately notify DWDAL and immediately change my password.

C. I will not share with anyone any other information regarding access to Confidential Data records maintained by DWDAL unless I am specifically authorized by DWDAL.

D. I will not request access to any Confidential Data unless such access is necessary for the performance of my official duties.

E. I will not disclose any Confidential Data to any parties who are not authorized to receive such information (including but not limited to relatives, friends, etc.) except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) involved.

F. I shall retain Confidential Data only for that period of time necessary to perform my duties or to comply with the purposes set forth in the Grant Award. Thereafter, I shall either arrange for the retention of such information consistent with federal record retention requirements or delete or destroy such data.

G. I have either been trained in the proper use and handling of Confidential Data or I have received written standards and instructions in the handling of such data. I shall comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which Confidential Data data may be kept; and c) following procedures for the timely disposal, destruction or deletion of Confidential Data.

H. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I further acknowledge that applicable state law may provide that any individual who discloses Confidential Data in violation of state law or regulation may be subject to a fine and/or a period of imprisonment and dismissal from public service. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.

I. Should I have any questions concerning the handling or disclosure of Confidential Data, I shall immediately notify DWDAL at danielle.cox@maryland.gov and be guided by advice given by DWDAL regarding the handling of Confidential Data.

Employee Signature: _____ Date: _____

Employee Name (printed): _____

Employer: _____

Address:

_____

_____

_____

Work Telephone: _____

E-Mail: _____

Attachment D

**Confidentiality Certification**
**For Access to**
**DLLR's Apprenticeship Confidential Data**

I understand that as a result of my employment I will or may be exposed to certain confidential information from records and systems maintained by the Maryland Department of Labor, Licensing and Regulation ("DLLR"). Such information, hereinafter referred to as "Confidential Data," may include, but is not limited to, names, addresses, social security numbers, birth dates, prevailing wage records, apprenticeship agreements and status, which information is private and confidential and may not be disclosed to others. That information may be kept in DLLR systems and files or in the United States Department of Labor RAPIDS system. I understand that this certification must be renewed periodically depending on the access I have been granted or requirements of DLLR or DOL. I acknowledge and agree to abide by the following standards for the receipt and handling of Confidential Data:

A. I shall not disclose my username (if applicable), password (if applicable), or any other information needed to access Confidential Data maintained by DLLR and DOL to any party nor shall I give any other individual access to this information.

B. If I should become aware that any other individual, other than an authorized employee, agent, contractor, or subcontractor of my employer, may have obtained or has obtained access to my username, password or other information needed to access records maintained by DLLR and DOL, I shall immediately notify DLLR and immediately change my password.

C. I will not share with anyone any other information regarding access to Confidential Data records maintained by DLLR and DOL unless I am specifically authorized by DLLR.

D. I will not request access to any social security numbers or wage data unless such access is necessary for the performance of my official duties.

E. I will not disclose any Confidential Data to any parties who are not authorized to receive such information (including but not limited to relatives, friends, etc.) except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) involved.

F. I shall retain Confidential Data only for that period of time necessary to perform my duties or to comply with the purposes set forth in the Agreement. Thereafter, I shall either arrange for the retention of such information consistent with federal record retention requirements or delete or destroy such data.

G. I have either been trained in the proper use and handling of Confidential Data or I have received written standards and instructions in the handling of such data. I shall comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which wage record data may be kept; and c) following procedures for the timely disposal, destruction or deletion of Confidential Data.

H. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I further acknowledge that applicable state and federal law may provide that any individual who discloses Confidential Data in violation of state law or regulation may be subject to a fine and/or a period of imprisonment and dismissal from public service. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.

I. Should I have any questions concerning the handling or disclosure of Confidential Data, I shall immediately notify DLLR at christopher.maclarion@maryland.gov and be guided by advice given by DLLR regarding the handling of Confidential Data.

Employee Signature: _____ Date: _____

Employee Name (printed): _____

# SECURITY BREACH

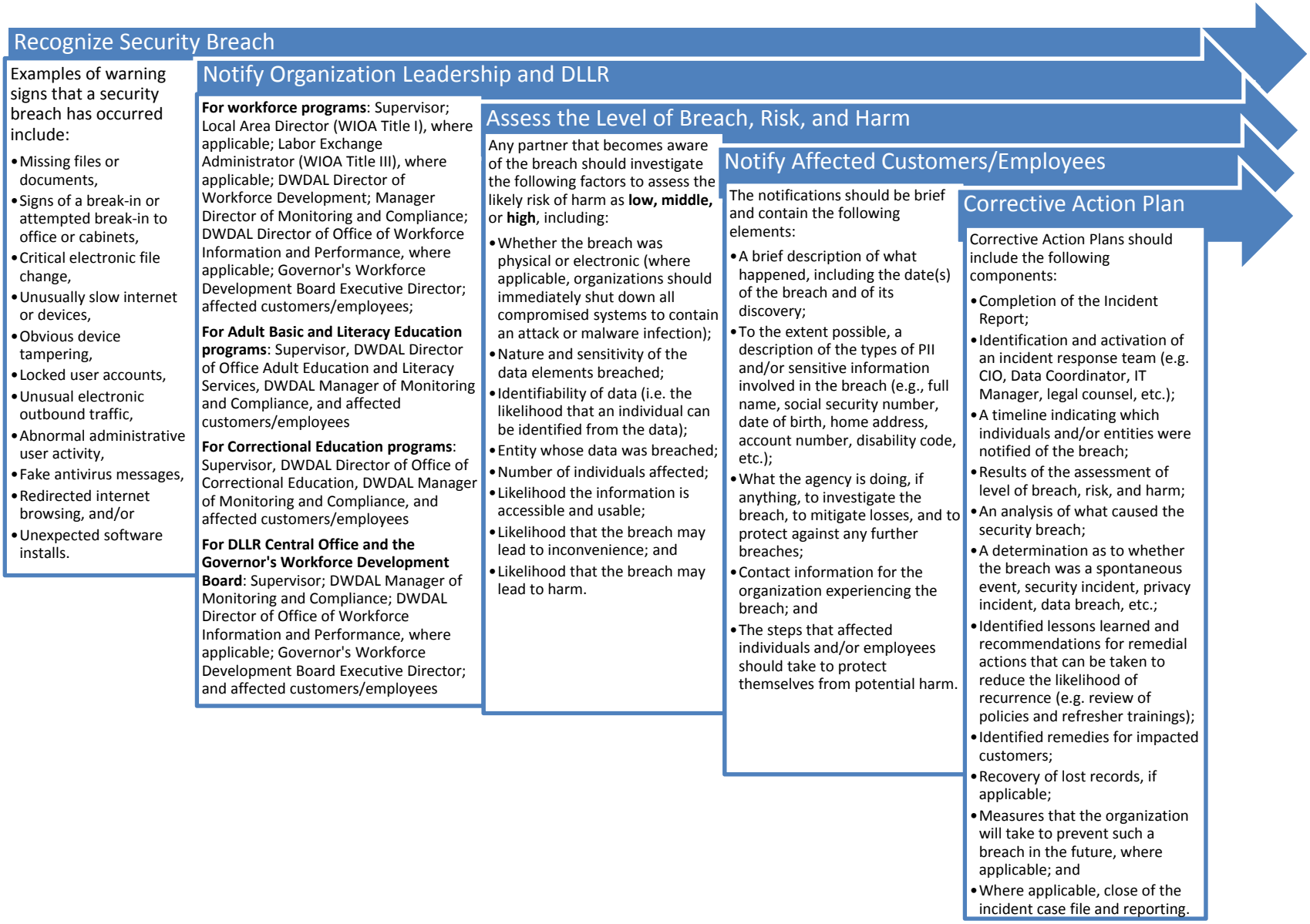
The term “breach” is used to indicate the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. Breaches can be the result of a spontaneous incident (e.g. data system error), security incident (e.g. break-in), privacy incident (e.g. failure to maintain confidentiality), staff error, data breach, etc. Breaches are hazardous both to customers and to organizations involved. Individual harm may include identity theft, embarrassment, or blackmail. Organizational harm may include a loss of public trust or legal liability.

Whether the breach occurred within local, State, or vendor records, the breached entity must notify the organizations and individuals, as outlined in the previous table within three business days. For each breach, the Department of Labor, Licensing and Regulation’s Division of Workforce Development and Adult Learning (DLLR’s DWDAL) Manager of Monitoring and Compliance must be notified as soon as possible. Entities must not wait to notify DLLR until after an investigation has been conducted, for timing is essential to resolving breach issues and protecting customers and employees. The Director, then, is in charge of notifying the USDOL Field Program Officer of the breach within 24 hours if the breach is assessed to have a high level of harm (high impact breach). The DLLR DWDAL Director of the Office of Workforce Information and Performance must be notified of any electronic breach that involves the MWE.

In a **low impact breach**, individuals or the organization may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).

In a **medium impact breach**, individuals or the organization may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.). They may lose capability of finishing or completing an activity as scheduled due to the physical or electronic PII breach (e.g. through identification of family status).

In a **high impact breach**, individuals or the organization may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.) or irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.). Examples of high impact breach include the possibility to cause harm such as blackmail, increase mental condition, defamation using person's name in precarious situations, physical harm, loss of benefits, harm to staff assisting clients, number of files or type of data breached.




Additional notifications may be required based on State and Federal laws as well as entities' data sharing agreements. This chart is not meant to define all the responsibilities an entity may have as a result of a breach or suspected breach but is meant to define partner's responsibilities to notify DWDAL.

# Sample Initial Incident Report

This document is only an initial report to be submitted to the Department of Labor, Licensing and Regulation (DLLR) upon the suspected occurrence of an incident. The State of Maryland or DLLR may make further requests for information if it deems it appropriate

1. **Date Incident(s) reported to Local agency**
2. **Parties associated with incident (name of company, or individual)**
3. **Parties affected by incident**
4. **Origin of the Incident (place, area or dept.)**
5. **Information Report By:**
   a. Name of Direct Contact
   b. Agency/Company
   c. Phone Number
   d. Date Reported (if different from above)

6. **Incident Information (answer in detail)**
   a. Type of Incident (physical or electronic):
   b. Functional Impact (High, Medium, Low):
   c. Information Impacted (Include sensitivity level):
   d. Likelihood of Recoverability of items:
   e. Level of Breach, Risk, and Harm:
   f. Estimated Date and time of Incident?
   g. Other parties notified of incident (date, name, title and location)
   h. When reporting party confirmed the incident?
   i. How was incident discovered?
   j. Location of the incident (w/address):
   k. What type of information was breached, tampered with, copied, forged, shredded?
   l. Were there contributors that caused the incident? If so, how?
   m. Did it involve a federally funded program? If so, which one?
   n. Did it involve fraud or theft of funds?
   o. Were there prior occurrences of similar incidents? If so, how many? When? By Whom?

7. **Notification and Interviews**
   a. Date and time reported to State.
      - Name of Agency:
      - Reported as what type of incident:
      - Name of Director and/or Manager(s) notified:

   b. Was law enforcement notified by reporting or local agency?
      - Law Enforcement Agency:
      - Date Notified to agency:
      - Report Number(s):
      - Name of Officer(s):

c. Was the information exposed internally and/or externally or both (detail)?
d. What were the initial actions taken by the reporting party or local agency (detail)?
e. Individual(s) Interviewed relating to incident (with dates and time)
f. If incident was under another source (not local entity), were interviews conducted with staff or parties involved? If so by whom and with what individuals (provide dates and time)? Provide conclusion report along with this form.

**8. Findings**

**Summarize in detail:**

***Note: If PII is involved, agencies may be requested to provide a list of impacted individuals along with appropriate contact information such as mailing address.***

**9. Conclusion/Remedy**

a. Remedy provided:
b. Are there legal actions taken (detail):
c. Measures or protection mechanism in place and/or enhanced to eliminate future incidents.
d. Policy Changes made (new security practices).
e. Who received Training? When?

***Note: Attached any pertinent information that will assist in our analysis and review of the reported incident.***

**Send Incident Reports to the Division of Workforce Development and Adult Learning to:**

Assistant Secretary;
Director of Workforce Development and
Monitoring and Compliance Manager
1100 N. Eutaw Street, Suite 108
Baltimore, Maryland 21201

**Please modify to fit your unique situation.**