



**Division of Workforce
Development and Adult Learning
(DWDAL)**
Policy Issuance



PI 2026-17 Privacy and Data Security | October 28, 2026

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	DWDAL Maryland Department of Labor (MD Labor)
SUBJECT	DWDAL Privacy and Data Security Policy
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 MD Labor 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.

QUESTIONS

Lauren Gilwee
Director, Policy
DWDAL
410.767.2268

lauren.gilwee@maryland.gov

Ruschelle Reuben
Director, Office of Correctional
Education
DWDAL
410.767.9769

ruschelle.reuben@maryland.gov

Rachael Stephens Parker
Executive Director, Governor's
Workforce Development Board
MD Labor
443.800.5702

rachael.parker@maryland.gov

Chris MacLarion
Director, Apprenticeship and Training
DWDAL
410.767.3969

christopher.maclarion@maryland.gov

Melissa Volpe, Acting Director
Office of Workforce Development
DWDAL
410.767.2995
melissa.volpe@maryland.gov

Perketer Tucker
Director, Office of Adult Education &
Literacy Services
DWDAL
410.767.4150

perketer.tucker@maryland.gov

Tanya Washington
Manager, Office of Monitoring and
Compliance
DWDAL
410.767.2098

tanya.washington@maryland.gov

Chad White
MWE System Administrator
DWDAL
410.767.2103

chad.white@maryland.gov

**PREPARED
BY**

Dylan McDonough, Senior Policy Analyst, DWDAL, MD Labor

TABLE OF CONTENTS

PRIVACY AND DATA SECURITY POLICY

CANCELLATIONS	4
EXECUTIVE SUMMARY	5
GENERAL INFORMATION	6
WORKFORCE INNOVATION AND OPPORTUNITY ACT	6
SENSITIVE AND PERSONALLY IDENTIFIABLE INFORMATION	6
FEDERAL ACTS ON PRIVACY AND DATA SECURITY	7
MARYLAND’S APPROACH TO DATA SECURITY	7
DWDAL’s Collection and Use of Data	8
DWDAL Data Systems	8
ACCESS TO DATA SYSTEMS	10
CUSTOMER RELEASE OF INFORMATION	10
DATA SHARING MEMORANDA OF UNDERSTANDING	10
STAFF ROLES & RESPONSIBILITIES	10
Data Training Responsibilities	11
PROTECTION OF DATA AND SENSITIVE INFORMATION	12
PHYSICAL DATA SECURITY REQUIREMENTS	12
Retention and Disposal of Physical Records	13
ELECTRONIC DATA SECURITY REQUIREMENTS	13
Retention and Disposal of Electronic Records	14
SECURITY BREACHES	15
RECOGNIZING A SECURITY BREACH HAS OCCURED	15
NOTIFICATION TO DWDAL	15
ASSESS THE LEVEL OF BREACH, RISK, AND HARM	17
CORRECTIVE ACTION PLAN	18
CONSEQUENCES OF NONCOMPLIANCE AND MONITORING	20
CONSEQUENCES OF NONCOMPLIANCE	20
Lack of Policy or Directives	20
Unauthorized Disclosure of PII and Sensitive Information	20
State and Federal Level of Failure to Address Security Breach	20
MONITORING	21
FAIR PRACTICES AND ACCESSIBILITY	22
REFERENCES	23
LAW	23
REGULATION	23
FEDERAL GUIDANCE	23
OTHER RESOURCES	23

CANCELLATIONS

The following policies are hereby cancelled and replaced by this policy issuance:

- Policy Issuance 2019-04, “Privacy and Data Security,” dated March 28, 2019.

Archived policies are available at: <http://www.labor.maryland.gov/employment/mpi/>.

EXECUTIVE SUMMARY

Maryland is committed to increasing the earning capacity of Marylanders, which will support businesses. This goal can only be achieved through working with agency partners within WIOA system, including the Maryland Department of Labor (MD Labor); Department of Human Services (DHS); Division of Rehabilitation Services, Department of Housing and Community Development (DHCD), Governor's Workforce Development Board (GWDB), and the Maryland Workforce Association (MWA). 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 MD Labor'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). 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 Personally Identifiable Information (PII) and sensitive information.

Protecting PII and sensitive information is a federal and State priority. PII is defined as participant-level and employee data that either by itself or combined with other data can link to a specific individual or identity. 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..

DWDAL administers a number of WIOA State Plan programs in which 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. The participant-level data collected helps the programs by allowing staff to better understand the individual's circumstances and how to best assist and support them in pursuing their workforce goals.

DWDAL warehouses data in two main data systems, the Maryland Workforce Exchange (MWE) and the Literacy, Adult and Community Education System (LACES). While the MWE and LACES are the division's two main data systems, smaller systems also exist such as the Apprenticeship Information Management System (AIMS), Correctional Education (CE) Student system, and the federal Registered Apprenticeship Partners Information Management Data System (RAPIDS). Any new functionality or systems incorporated into the system are covered by this policy. Though much of the participant-level data collected is stored electronically, in some cases, there may be cases where staff handles physical forms of PII and sensitive data (paper files).

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.

In the event of a security breach the appropriate people must be notified immediately and staff must assess the magnitude of the breach before implementing the Corrective Action Plan.

GENERAL INFORMATION

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 and amends the Adult Education and Family Literacy Act, the Wagner-Peyser Act, and the Rehabilitation Act of 1973. To help both businesses and job seekers meet their needs, the workforce system established under WIOA is integrated by design. 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 by 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.

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 nonsensitive 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 itself, could not reasonably be expected to result in personal harm. It is stand-alone information	Examples of non-sensitive PII include information such as first and last names, email addresses, business addresses, business telephone numbers, general education

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. § General Provisions 4-101(f) (vii) defines "telephone number" as personal information. COMAR 09.01.04.13A(3) includes "personal phone number" as sociological information.

Type of Data	Definition	Examples
	that is not linked or closely associated with any protected or unprotected PII.	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 laws³ exist to ensure customer data protection, including:

1. The Privacy Act of 1974;
2. The Family Educational Rights and Privacy Act (FERPA);
3. The Health Insurance Portability and Accountability Act (HIPAA); and,
4. 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 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 (UI) program, and its corresponding regulations define and protect the confidentiality of unemployment records.

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)⁴ 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.⁵ Both statutes contain notification requirements under certain circumstances.

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 Md. Code Ann. Comm. Law §§[14-3501](#) *et seq.*

⁵ Md. Code Ann. State Gov't §[10-1301](#) *et seq.*

Maryland is committed to increasing the earning capacity of Marylanders, which will support businesses. This goal can only be achieved by partnering with other agency partners within the WIOA system, including DHS; the Division of Rehabilitation Services, DHCD, GWDB, and MWA. 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 MD Labor's DWDAL-specific data, as well as in handling partner data attained through Data Sharing MOUs. 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 Workforce Development Areas (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.

DWDAL'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 (JVSG); the Senior Community Service Employment Program (SCSEP); 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:

1. Determine eligibility for participation in WIOA programs;
2. Determine eligibility for inclusion on Maryland's Eligible Training Provider List ETPL;⁶
3. Determine barriers to employment and provide supportive services, where applicable;
4. Track and ensure that programs (including State and local partners) are helping customers as they are intended to do;
5. Track performance metrics;
6. Track co-enrollment of customers;
7. Track follow-up with customers;
8. 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);
9. Help Maryland understand the state of the workforce system; and,
10. 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).

⁶ For more information on Maryland's Eligible Training Provider List, see DWDAL Policy Issuances, available at: <https://labor.maryland.gov/employment/mpi>

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, JVSJ), 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 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. DHS 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.⁷ 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 (MATP) 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 data, while housed in LACES, is also linked to and subject to rules and regulations of the Department of Public Safety and Correctional Services.⁸ Any new functionality or systems incorporated into the system are covered by this policy.

⁷ Temporary Assistance for Needy Families (TANF), Vocational Rehabilitation, and Community Service Block Grant 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.

⁸ 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

CUSTOMER RELEASE OF INFORMATION

The MWE includes a customer disclaimer, which allows for the sharing of performance data between DWDAL and approved partner agencies.⁹ 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 MD Labor DWDAL and the MD Labor MDUI have a Data Sharing MOU in place that gives DWDAL access to certain 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 Area must have a MOU in place with MD Labor, 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 MD Labor.¹⁰

MD Labor is currently in the process of incorporating the 2024 State Wage Interchange System (SWIS) into the MWE system. In the interim, all partners must ensure they are following State Workforce Innovation System (SWIS) guidelines¹¹ for PII related to wage data.

STAFF ROLES & RESPONSIBILITIES

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

1. 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.

⁹ A list of the partner agencies covered by the MWE disclaimer can be accessed by contacting the MWE Help Desk.

¹⁰ This is not an all-inclusive list of MOUs in place between MD Labor and its partners. This policy covers all current and future Data Sharing MOUs with MD Labor.

¹¹ More information and guidance on the SWIS can be found at the following link:
<https://www.dol.gov/agencies/eta/performance/swis>

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

Table 2: Staff Confidentiality Agreement by Data System

Data System	Agreements are Submitted To
MWE ¹²	Director, Office of Workforce Development
LACES	Director, Office of Adult Education & Literacy Services
Correctional Education Student Database	Director, Office of Correctional Education
RAPIDS or AIMS	Director, Apprenticeship and Training

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. MD Labor 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, physical files, and electronic data systems. Training may be conducted online and/or combined with other ethics training (e.g. ethics with handling UI data).

¹² Individuals with access to the MWE system that are not employed by the MD Labor central office should follow DWDAL policy issuance “Partner Access to the Maryland Workforce Exchange (MWE)” in submitting their Staff Confidentiality Agreements. DWDAL current and archived policy issuances are available online at: <https://labor.maryland.gov/employment/mpi/>

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. While neither physical nor electronic, staff must also maintain verbal protection¹³ 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:

1. Reducing the volume of collected and retained physical data to the minimum necessary as is needed for reporting, eligibility determination, and case management;
2. Limiting access to those individuals who must have access to perform job functions;
3. Keeping files in cabinets and offices that lock;
4. 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;
5. 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;
6. Developing and adopting a risk-aware culture;
7. Conducting due diligence on all third-party service providers and requiring appropriate information security standards to be written into contracts;
8. Conducting on-hire and annual training on the protection of physical data;
9. Developing a data governance policy and/or procedures;
10. Developing and testing an incident response plan, which should involve key stakeholders;¹⁴
11. Using unique identifiers to de-identify records and remove PII (e.g. new unique number specific to organization versus use of social security number);
12. Using locked boxes when transferring data for auditing; and,
13. Using confidential recycling to dispose of records.

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

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

¹³ When interacting with clients, staff must take reasonable steps to ensure privacy when PII must be shared verbally.

¹⁴ 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. MD Labor 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:

1. Reducing the volume of collected and retained electronic data to the minimum necessary;
2. Limiting data access to only those individuals who must have such access;
3. Using password-protection, encryption-preferred,¹⁵ 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 access¹⁶);
4. 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;
5. Ensuring that data is not left unattended (e.g. MWE data must not be left open on screen while on a lunch break);
6. Logging out of data systems when leaving one's desk;
7. Limiting network access to approved devices certified with appropriate security controls;
8. Not accessing data systems from non-secure computers (e.g. personal computer);
9. Conducting due diligence on all third-party service providers and requiring appropriate information security standards to be written into contracts;
10. 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;
11. Conducting on-hire and annual training on the protection of electronic data; Developing a data governance policy and/or procedures;
12. Developing and testing an incident response plan, which should involve key stakeholders; and,
13. When receiving data requests:

¹⁵ 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.

¹⁶ 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.

- a. Providing aggregate-level data (i.e. all PII and sensitive information removed and performance numbers combined to represent the whole program or class); or,
- b. 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:

1. Setting computers to go to screensaver after a maximum of five minutes of inactivity;
2. Setting computer to lock after a maximum of 15 minutes of inactivity;
3. Developing and maintaining access by documenting and reviewing users and roles regularly;
4. Blocking PII and sensitive information from being downloaded to individual devices (e.g. flash drive);
5. Developing and maintaining an inventory of all hardware and software;
6. Using the most current versions of applications and operating systems;
7. Requiring complex passwords and using multi-factor authentication;
8. Developing and adopting a risk-aware culture;
9. Conducting vulnerability testing and risk assessments;
10. Investing in cyber insurance;
11. 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,
12. 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. 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.¹⁷

¹⁷ 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 PII, whether physical or electronic.¹⁸ 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.

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:

1. Missing files or documents;
2. Signs of a break-in or attempted break-in to office or cabinets;
3. Critical electronic file change;
4. Unusually slow internet or devices;
5. Obvious device tampering;
6. Locked user accounts;
7. Unusual electronic outbound traffic;
8. Abnormal administrative user activity;
9. Fake antivirus messages;
10. Redirected internet browsing; and/or,
11. 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 supervisor. The table below outlines which entities need to be notified¹⁹ at a minimum, by type of program, in the event of a breach:

¹⁸ Office of Management and Budget, Memorandum 07-16, “[Safeguarding Against and Responding to the Breach of Personally Identifiable Information](#),” dated May 22, 2007.

¹⁹ 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.

Table 3: Notification Parties in the Event of a Breach

Workforce Program	Strategic Initiatives	Adult Basic and Literacy Education Program	Correctional Education Program	MD Labor Central Office and GWDB
<ol style="list-style-type: none"> 1. For WIOA Title I, Local Area Director (or designee); 2. For WIOA Title III, Reemployment Program Director; 3. DWDAL Director of Workforce Development; 4. DWDAL Manager of Monitoring and Compliance; 5. DWDAL MWE Systems Administrator, where applicable; 6. Affected customers/employees; and, 7. GWDB Executive Director. 	<ol style="list-style-type: none"> 1. DWDAL Director of the Office of Strategic Initiatives; 2. DWDAL Manager of Monitoring and Compliance; 3. Grantee programs; and, 4. Affected customers/employees. 	<ol style="list-style-type: none"> 1. DWDAL Director of Office Adult Education and Literacy Services; 2. DWDAL Manager of Monitoring and Compliance; 3. Grantee programs; and, 4. Affected customers/employees. 	<ol style="list-style-type: none"> 1. DWDAL Director of Office of Correctional Education; 2. DWDAL Manager of Monitoring and Compliance; and, 3. Affected customers/employees. 	<ol style="list-style-type: none"> 1. DWDAL Manager of Monitoring and Compliance; 2. DWDAL MWE Systems Administrator, where applicable; 3. DWDAL Assistant Secretary; 4. Secretary of MD Labor; 5. Affected customers/employees; and, 6. GWDB Executive Director.

Additionally, all parties must comply with the State of Maryland Department of Information Technology's IT Security Manual and all relevant policies on Cybersecurity. These policies may be found on the Department of Information Technology's website:
<https://doit.maryland.gov/policies/ci/Pages/default.aspx>.

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 MD Labor DWDAL Monitoring and Compliance Manager must be notified as soon as possible. Entities must not wait to notify MD Labor until after an investigation has been conducted, for timing is essential to resolving breach issues and protecting customers and employees. The MD Labor 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 MD Labor DWDAL System Administrator for the MWE and Performance Unit must be notified of any electronic breach that involves the MWE.

The notifications should be brief and contain the following elements:

1. A brief description of what happened, including the date(s) and rough time estimate(s) of the breach and of its discovery;
2. 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.);
3. What the agency, organization, or entity is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches;
4. Contact information for the organization's person of contact leading the efforts for the investigation; and
5. 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.

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:

1. Whether the breach was physical or electronic (where applicable, organizations should immediately shut down all compromised systems to contain an attack or malware infection);²⁰
2. Nature and sensitivity of the data elements breached; Identifiability of data (i.e. the likelihood that an individual can be identified from the data);
3. Entity whose data was breached;
4. Number of individuals affected;
5. Likelihood the information is accessible and usable;
6. Likelihood that the breach may lead to inconvenience; and,
7. 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.).

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

²⁰ 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.

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.). High impact breaches can be identified by the number of files or the type of data that has been breached. Examples of a high impact breach include the possibility to cause harm such as blackmail, defamation using a person's name in precarious situations, mental or physical harm, loss of benefits, or harm to staff assisting clients.²¹

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 System Administrator for the MWE and Performance Unit, 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:

1. Completion of the Incident Report;
2. Identification and activation of an incident response team (e.g. CIO, Data Coordinator, IT Manager, legal counsel, etc.);
3. A timeline indicating which individuals and/or entities were notified of the breach; Results of the assessment of level of breach, risk, and harm;
4. An analysis of what caused the security breach;
5. A determination as to whether the breach was a spontaneous event, security incident, privacy incident, data breach, etc.;
6. 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);
7. Identified remedies for impacted customers;
8. Recovery of lost records, if applicable;
9. Measures that the organization will take to prevent such a breach in the future, where applicable; and,
10. Where applicable, close of the incident case file and reporting.

²¹ 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.

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 (LWDB) 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

MD Labor 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 MD Labor may take the following actions:

1. Send a warning letter of noncompliance;
2. Remove or restrict access to PII and sensitive information in physical files and/or data systems;
3. Send a letter of noncompliance to alert and mobilize the GWDB and the MD Labor Secretary's Office for further action;
4. Request action before providing funding; and/or,
5. 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 MD Labor 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.

FAIR PRACTICES AND ACCESSIBILITY

It is MD Labor's policy that all persons have equal opportunity and access to services and facilities without regard to race, religion, color, sex (including pregnancy, childbirth and related medical conditions, transgender status, gender identity, and sexual orientation), marital status, genetic information, age, national origin or ancestry (including Limited English Proficiency), disability, veteran status, political affiliation or belief, for the beneficiaries, applicants, and participants only, on the basis of citizenship status, or participation in a program or activity that receives financial assistance under Title I of WIOA. Interested parties may refer to MD Labor's Nondiscrimination Plan²² and Language Access Plan²³ for more information on accommodations and services.

²² MD Labor's Nondiscrimination Plan is available at the following link:

<http://www.labor.maryland.gov/employment/ndp/>.

²³ The DWDAL and UI Language Access Plan is available at the following link:

<http://www.labor.maryland.gov/employment/wioa-access.pdf>.

REFERENCES

LAW

- [Workforce Innovation and Opportunity Act](#), 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;
- 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 ([Unemployment Insurance Penalties](#));
- Md. Code, State Gov't Art. §§ 10-1301 *et seq.* ([MD Government Info Protection](#)) as amended;
- Md. Code, Crim. Law § 7-302 ([MD Unauthorized Computer Access](#)) ;
- Md. Code, Crim. Law § 8-606 ([MD Fraud & False Records](#)) as amended.

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;
- SWIS Amendments, accessed July 10, 2025, <https://www.dol.gov/agencies/eta/performance/swis>
- Office of Management and Budget Memorandum 07-16, "[MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES](#)," 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.