TITLE: Administrative Policy #3025R1
Data Security and Personally Identifiable Information

Administrative Policy

Date Established: 02/14/2020
Date Last Revised: 8/11/2022
Date Posted to Website: 4/27/2020
Status: Final
Supersedes: 3025

Purpose

To establish methods of compliance, security, and integrity within the computer network systems and media storage that PacMtn staff and agents use in the course of service delivery and administration of local, state, and federal programs. Maintenance to secure sensitive and protected information as well as Personally Identifiable Information (PII) of program participants is of the utmost critical nature. All data storage, exchange, and disposition will follow strict rules to ensure compliance with applicable program, state, and federal regulations.

Policy

PacMtn, in coordination with other State Agencies and organizations in which shared networks areestablished, will implement, and follow guidance on all data security requirements.

PacMtn maintains a computer network that restricts access to only staff and approved contracted staff. Unique user profiles and passwords are created for each user upon hire and access is limited toonly applicable files and rights necessary to fulfill job requirements.

Administrative access to the network is limited to contracted IT vendors and a staff member who oversees daily oversight of users. If PacMtn staff will be using networks other than those maintainedby PacMtn, all processes and forms required by the applicable hosting agency will be followed and documented with approvals from program supervisors.

Oversight and review of access to networks will be done regularly through account reports. Access to outside networks will be reviewed annually via reports from applicable agencies to confirm only authorized users are listed. Access to networks or specialized software can be removed immediatelyupon request.

Staff shall not share access with unauthorized users nor share access information between other staff. Any staff who violates this, circumvents security, or otherwise puts the network or data at riskwill be at a minimum required to go through training, but further disciplinary action, up to termination may occur depending on the severity of the violation.

Program requirements may sometimes include the gathering and storing of data that is highly confidential (Category 4 data). All program staff that may come in contact with such data must go through training on the applicable requirements as set forth by federal and state regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), Pub.

L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act(FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFRPart 2; and/or Criminal Justice Information Services, 28 CFR Part 20. Data of this nature shall onlybe stored on approved networks and software as provided by and secured by the agency that requires it. Furthermore, access to software and databases that house this information shall require additional approvals and training by the governing agency per their policies.

Policy Guidelines

1. Definitions:

Personally identifiable information (PII) -

1. Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples include, but are not limited to name, address, phone number, email address, social security number, passport number, driver's license or state identification card information, date and place of birth, mother's maiden name, or biometric records; and
2. Any other information that is linked or linkable to an individual such as medical, educational, financial, demographic, gender, race, and employment information. Images disclosing physical characteristics, photographic image, fingerprints, retinal scans, or voice signature in any medium and from any source, are also considered PII.

Breach - Actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, and/or any similar occurrence where:

1. A person other than an authorized user accesses or potentially accesses PII, or
2. An authorized user accesses or potentially accesses PII for other than authorized purposes.

Security incident - A set of events that have been examined and determined to indicate a violation of security policy or an adverse effect on the security status of one or more systems within an organization or entity.

2. Administrative Controls

PacMtn is committed to ensuring the integrity and security of its networks and the data stored therein. Administrative controls are documented in this policy to provide the necessary requirementsto follow to maintain that integrity. Additionally, further risk assessments will be for any new system(s) housing Category 4 Data.

2.1 Authorization, Authentication and Access

Controls and processes have been established to limit access to networks and files containing sensitive data and to secure authorization procedures to maintain security at all times.

Controls in place include:

a. Restricted access of administrative functions to authorized staff such as contracted vendoror staff maintaining the network.
b. Restricted access of users to staff or contracted staff as authorized via email or Microsoft planner. The contracted staff authorization email must be approved by a supervisor or higher.
c. User accounts are unique and allows for tracking of actions made.
d. User/employee's access to the network/Data is suspended immediately:
    1. Upon suspected compromise of the user credentials.

2. When their employment, or the contract under which the Data is made available to them, is terminated.
3. When they no longer need access to the Data to fulfill the requirements of the contract.

e. Periodic reviews of network users and access levels, both internal and users on external networks housing the data.

f. Password restrictions and logon requirements
   1. Passwords will have a minimum length of 8 characters and contain at least three ofthe following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.
   2. The password must not contain a user's name, logon ID, or any form of their full name.
   3. The password should not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.
   4. Passwords must also be significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.

g. If Personally Identifiable Information (PII) or any other confidential information needs to be accessed from an external location (the Data will traverse the Internet or otherwise traveloutside the network), additional security measures are required to mitigate risk.
   1. Ensuring mitigations applied to the system don't allow end-user modification.
   2. Not allowing the use of dial-up connections.
   3. Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.
   4. Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must always beencrypted while traversing any network, including the Internet, which is not a Trusted Network.
   5. Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.
   6. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition,iris scan) or token (software, hardware, smart card, etc.) in that case:
      1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor.
      2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)
      3) Must not contain a "run" of three or more consecutive numbers (12398, 98743 would not be acceptable)

h. If PII or any other confidential information is stored on a Mobile Device, passcodes used onthe device must:
   1. Be a minimum of six alphanumeric characters.
   2. Contain at least three unique character classes (upper case, lower case, letter, number).
   3. Not contain more than three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.
   4. Render the device unusable after a maximum of 10 failed logon attempts.

3. <u>Protection of Data</u>

Confidential client PII and data shall only be stored within the applicable MIS database systems as allowable and required by the awarding agency. No sensitive data will be stored on the local workstation hard disks or in shared folders within the network. Workstation access is limited to authorized users and requires unique identification and passwords. If sensitive, confidential participant data is provided in hard copy or paper form, all records shall be maintained in a separate, secure, locked, cabinet in an area that does not allow public access. Only authorized users will haveaccess to these areas. If PacMtn staff use portable electronic devices to gather and record information the device itself should be maintained in a secure area to avoid unauthorized access. Each portable device will be password protected, and data should not be stored on the device harddrive.

4. **System Protection**

Ongoing protection of the system is required to prevent compromise of the network and data. In order to maintain system protection, the following protocols are required:

a. Systems must have all security patches or hotfixes applied within 3 months of being made available.
b. The contracted IT vendor or person responsible for maintaining the network will tracksecurity patches and hotfixes and document required timeframes and subsequent installations.
c. Systems shall have an Anti-Malware application, if available, installed.
d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and anymalware database the system uses, will be no more than one update behind the current.

5. **Data Segregation**

a. PacMtn provides services to multiple programs representing a variety of state and federal funders. These programs have unique MIS databases in order to track and secure participantdata. These databases are separate from the general network storage. Only program and participant information applicable to each shall be maintained in the respective databases.
b. If for any reason data from multiple programs is in the same database or is available withinthe same network outside of a database, every attempt should be made to segregate to the highest extent possible. This includes unique identifiers within the records of a database. Security requirements of the most restrictive program will be maintained in such event.
c. When documents are stored as physical paper documents, data will also be physically segregated by means of separate drawers, files, or other containers.

6. **Data Disposition**

When the contracted work has been completed or when the data is no longer needed, data shall be returned to the applicable agency or destroyed. Media on which data may be stored and associated acceptable methods of destruction are as follows

Data stored on	Will be destroyed by
Server or workstation hard disks, or Removable media (e.g., floppies, USB flash drives, portable harddisks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g., CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive; Magnetic tape; Degaussing, incinerating or crosscut shredding

7. <u>Data shared with or by a Contract holder or Subcontractors</u>

A. The service provider will only share data with organizations who have an active grant or contract with the service provider, for whom the service provider is a grantee, or where a valid data sharing agreement exists between all parties.
B. Only data necessary for the purposes of carrying out a grant or contract will be shared with grantors, grantees, contractors, or partners.
C. All data created or obtained by a service provider for the purposes of carrying out a grant or contract awarded by PacMtn must be stored securely within a system that meets the security requirements of this policy. Data stored on a shared network that is considered category 3 or 4 and that may not be accessed by any user who isn't explicitly authorized to access it, must be stored in a secure fashion by password protecting the document containing the information. Sharing data owned by the subrecipient or obtained from the PacMtn must only be done so with individuals authorized to access the data.
D. If program, program applicant and/or program participant data is to be shared by a Contract Holder or with a Subcontractor, the specific Contract must include or refer to and follow the data security provisions of this policy. As applicable, the data security provisions held by the Contract Holder will be included within the Contract and adhered as allowable and or required by local, state, or federal requirements. This would also apply to any amendments, attachments, or exhibits within or as part of the Contract. If the Contractor cannot protect the data as articulated within this policy and as written within the Contract, then the contract must be submitted to the applicable head agency Contact specified for the contract for review and approval.

8. <u>Security awareness</u> (ESD WorkSource Policy 1026)

A. Notification of access to confidential information
    1. Service provider employees who have access, or are expected to have access in the future, to sensitive, confidential, proprietary, or private data, must be advised of the following:
        a. The confidential nature of the information,
        b. The safeguards required to protect the information,
        c. The expectation that the employee only access or store information that is necessary for their official duties, and
        d. There are civil and criminal sanctions for noncompliance that are contained in the Privacy Act of 1974 and other Federal and state laws.

2. Employees, before being granted access to confidential information, must acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.

B. Security awareness training – all service provider staff must receive security awareness training upon hire and annually. New hire training must include the risks of data compromise, an employee's role in prevention, and how to respond in the event of an incident.

9. Notification of Compromise or Potential Compromise

In the event of unauthorized data acquisition or disclosure that compromise or potentially compromises the security, confidentiality, or integrity of confidential information maintained, sharedwith or by PacMtn WDC, PacMtn staff, a Contract Holder, or a Subcontractor, PacMtn WDC will report to the applicable program/agency contact designated in the contract within one (1) business day of discovery.

Employment Security Department (ESD)

As required in Washington State WorkSource Policy 1026 – Safeguarding Personally Identifiable Information (PII), any breach or suspected breach of PII must immediately be reported to the Employment Security Department (ESD) at SystemPolicy@esd.wa.gov using "PII Incident" in the subject line. For grants managed by ESD, such as WIOA Title III, service providers must also follow ESD HR Policy 0031-1. This notification must include the following content:

- Workforce Development Area (WDA)
- Reporting Entity-LWDB, subrecipient, contractor, other and contact information
- Date of Incident
- Date of Discovery (if different)
- Number of files breached or affected
- Type of Issue:
    - o Hard copy files or information
    - o Electronic files or information
- Description of the incident
- Initial Determination of level of incident: o Carelessness
    - o Negligence
    - o Fraud
    - o Theft
    - o Other
- Any other relevant information
- If staff member is also an ESD employee, please refer to ESD HR Policy 0031-1-Security Breach Notification;
- If a Social Security Administration (SSA) related data breach/security incident, include **"SSA"** in the title;
- If ESD equipment loss or theft is involved, ESD staff must complete a Security Incident Report

Department of Social and Health Services (DSHS) data, if no contact is designated in the contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification orother requirements imposed by law or DSHS.

9.1 PacMtn WDC will promptly address and respond as follows:

1. Any PacMtn WDC, Contract Holder, or a Subcontractor staff member who discovers or is otherwise notified of the security breach will immediately inform PacMtn's Chief Financial and Administrative Services Officer.
2. A risk assessment will be conducted immediately following discovery of the data breach inorder to identify the root cause(s). Results of the risk assessment will be used to strengthensecurity protocols to ensure future data breaches do not occur.
3. In the event of a security breach where any personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information wasnot secured, PacMtn WDC shall notify the owner of the information of the potential or confirmed breach of the system immediately following discovery.
4. This notification must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after discovery of the breach. If necessary, notification may be delayed only long enough for PacMtn WDC to determine the scope ofthe breach and restore the reasonable integrity of the data system.
5. Delay may also occur if PacMtn WDC deems it necessary to contact the applicable law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation.
6. Notification may be provided by written or electronic notice. Electronic notice must be consistent with provisions regarding electronic records and signatures set forth in 15 U.S.C.Sec 7001.

   Both written and electronic notices must meet the following requirements:

   a. Written in plain language;
   b. Identify the PacMtn WDC as the reporting agency and include contact information;
   c. Include a list of the types of personal information that were or are reasonably believed to have been the subject of the breach;
   d. Include a time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
   e. Include toll-free telephone numbers and addresses of major credit reporting agencies.
7. As recommended in Training and Employment Guidance Letter (TEGL) 39-11, any breachor suspected breach of confidential personal information associated with an ETA funded grant must immediately be reported to the Federal Project Officer responsible for the grantand to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.
8. As required in RCW 19.255.010, any incident involving more than five hundred Washington state residents as a result of a single breach requires that PacMtn WDC to notify the Washington state attorney general of the breach no more than thirty days after the breach was discovered.

   This notification must include the following:

   a. The number of Washington state residents affected by the breach, or an estimate if the exact number is not known;
   b. A list of the types of personal information that were or are reasonably believedto have been the subject of the breach;
   c. A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;
   d. A summary of steps taken to contain the breach; and
   e. A single sample copy of the security breach notification, excluding any

personally identifiable information.

Note: the notice to the attorney general must be updated if any of the information identifiedabove is unknown at the time notice is due.

10. Security violation categories – based on review of the investigation items above, PacMtn WDC will categorize a violation as follows:

1. **Category 1 violation** – actions which violate federal, state, or local laws and regulations, including but not limited to:
    b. Unauthorized disclosure of protected health information or personal information in violation of privacy laws, including Washington state identity theft protection laws.
    c. Use of data to threaten, harass, or intimidate others.
    d. Engagement in illegal activities using data or information systems.

2. **Category 2 violation** – Category 2 violations involve breaches of this policy or related procedures but do not contravene federal, state, or local laws and regulations. Examples include, but are not limited to:
    a. Excessive or improper use of service provider data or information systems for personal reasons, such as excessive personal email or internet use, or visiting potentially harmful websites.
    b. Unauthorized attempts to bypass security controls, such as disabling anti-malware software or firewalls, sharing usernames and passwords, or delaying software updates.
    c. Viewing, displaying, or storing offensive, threatening, sexually explicit, obscene, or otherwise inappropriate content that contravenes the service provider's harassment policy.

11. Corrective action guidelines – Corrective actions for violations will be determined based on the category assigned and are outlined as follows:

1. **Corrective Actions for Category 1 Violations** – Violations in this category may require:
    a. Notification of relevant law enforcement agencies, regulatory bodies, and affected individuals.
    b. Revocation of access to the service provider's network or other involved data systems.
    c. Additional training on security and privacy practices.
    d. Disciplinary measures or termination of employment

2. **Corrective Actions for Category 2 Violations** – Violations in this category may result in:
    a. Issuance of a formal warning regarding breach of policy or procedures.
    b. Requirement for additional training on security and privacy practices.
    c. Revocation of access to the service provider's network or other involved data systems.
    d. Disciplinary action or termination of employment.

References

Health Insurance Portability and Accountability Act (HIPAA),
Pub. L. 104-191 as amended by the Health Information Technology for Economic and ClinicalHealth Act of 2009 (HITECH)
45 CFR Parts 160 and 164;

20 U.S.C. §1232g & 34 CFR Part 99 - The Family Educational Rights and Privacy Act (FERPA)Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf);
42 CFR Part 2 - Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records,
28 CFR Part 20 - Criminal Justice Information Services
within an organization or entity.
20 CFR 683.220
2 CFR 200.303
ESD Policy 1027
Guidance on the Protection of Personal Identifiable Information | U.S. Department of Labor (dol.gov)
Training and Employment Guidance Letter (TEGL) 39-11 - Guidance on the Handling and Protection of Personally Identifiable Information (PII)
RCW 19.255.010 - Personal information—Notice of security breaches
WorkSource Information Notice (WIN) 0109R7 - WIOA Title I-B verbal self-attestation and remote eligibility documentation and registration requirements during the COVID-19 emergency.

DATE APPROVED: February 14, 2020, 5/19/2021, 10/11/2021, 8/11/2022, 9/26/2024

Direct Inquiries to:
201 5th Ave., SW., Suite 401
Olympia, WA 98501
Telephone: (360) 515-5134
Email: Info@pacmtn.org

PacMtn is an equal opportunity employer/program. Auxiliary aids and services are available upon request toindividuals with disabilities. WA Relay 711