EMPLOY MILWAUKEE POLICY

POLICY: 21.02

SUBJECT: DATA SECURITY POLICY

ISSUANCE DATE: 8/26/21
EFFECTIVE DATE: 8/26/21

REFERENCES:

POLICY SCOPE

- ☒ EMPLOY MILWAUKEE AGENCY
- ☒ WIOA WDA 2 SYSTEM
- ☒ WIOA TITLE I-B PROGRAM(S)
  - ☒ ADULT PROGRAM
  - ☒ DISLOCATED WORKER PROGRAM
  - ☒ YOUTH PROGRAM
- ☒ NON-WIOA PROGRAMS

I. BACKGROUND

Information, including information entrusted to Employ Milwaukee by its clients, donors and business partners must be protected by taking reasonable and appropriate steps to ensure information's confidentiality, integrity, and availability. All members of the Employ Milwaukee workforce and all information systems used by Employ Milwaukee are required to comply with the information security policies.

II. PURPOSE

Employ Milwaukee collects and manages wide-ranging data and personally identifiable information (PII) through various activities and requirements. The purpose of this policy is to ensure that Employ Milwaukee's handling of data is consistent both internally and with its partners and in line with legal requirements.

III. POLICY

Acceptable use of assets

Information systems owned and provided by Employ Milwaukee are to be used for business purposes only. Information systems may not be used for the purpose of defamation, harassment, impersonation, forwarding of chain letters, personal purchases, etc.

Employ Milwaukee reserves the right to monitor, filter, and deny the use of its assets.

Use of Communications Services and Equipment

The communications services and equipment utilized by Employ Milwaukee are to be used primarily for legitimate and substantial business purposes. Personal use should be kept to a minimum. Personnel have a right to expect that other Employ Milwaukee personnel will not gain access for files, messages, communications, or documents of others unless they have a legitimate reason to do so. Accessing files, messages, communications, or documents of others without a legitimate reason is inappropriate and is prohibited.

Personnel must not utilize the communications services and equipment used by Employ Milwaukee in any way that may be seen as insulting, disruptive, or offensive to other persons, or harmful to morale. Examples of forbidden transmissions include sexually-explicit messages, cartoons, or jokes; ethnic or racial slurs; or any other message that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, religious beliefs, or other personal characteristics or circumstances.

Policy Violation

Any personnel who is found, after appropriate investigation, to have violated this policy will be subject to appropriate disciplinary action, up to and including termination.

Usage of Internet Access Systems

Employ Milwaukee provides Internet access to personnel. The guidelines listed below help personnel determine proper Internet usage. Employ Milwaukee reserves the right to monitor and record Internet usage and file server utilization of all personnel. This monitoring includes determining web sites visited and mail transmissions sent. Employ Milwaukee reserves the right to suspend individual user accounts for violation of Employ Milwaukee polices.

The following guidelines define Internet usage:

1. File transfers are to be for business use only by authorized Employ Milwaukee personnel.
2. Use of another person's account or access to their personal files without their consent is strictly prohibited.
3. Account passwords must be carefully protected to avoid the possibility of unauthorized use or intrusion of Employ Milwaukee systems. If a computer is lost or stolen, or if an ID or password are suspected to be stolen, report this immediately to management or designated IT personnel.
4. Confidential information is not to be transmitted without proper encryption.
5. All news group postings are to be for Employ Milwaukee business. Every message posted bears the address of Employ Milwaukee and therefore should be worded in such a way to promote and protect the integrity of Employ Milwaukee, and the confidentiality of its clients and donors.
6. Disruptive behavior such as introducing viruses or intentionally destroying or modifying files on the network is strictly prohibited.
7. Any personal use for commercial or illegal activity is strictly prohibited.

Downloading Files

1. All downloaded files or applications are to be scanned for viruses before being saved on Employ Milwaukee computers.
2. All downloaded applications must be approved by Employ Milwaukee's designated IT personnel before being installed on Employ Milwaukee computers.
   Exploration and use of the Internet pertaining to non-work related items should not interfere with productivity and must be done during lunch or break periods, or before or after work hours. Transmission of harassing, discriminatory or otherwise objectionable e-mail or files (as determined by the recipient) is strictly prohibited. Access to obscene or offensive sites is strictly prohibited and subject to disciplinary action.

Software Copyright Infringement

Employ Milwaukee licenses the use of computer software from a variety of outside companies. Employ

Milwaukee does not own this software or related documentation and, unless authorized by the software developer, does not have the right to reproduce it. Any duplication of licensed software, except for backup purposes, is a violation of the Federal Copyright Law which states that reproduction of software can be subject to civil damages up to $100,000 and criminal penalties, including fines and imprisonment.

Any personnel found copying software, for other than backup purposes, is subject to termination. Any staff member giving software to any outside third party, including clients or donors, or installing Employ Milwaukee software on non-Employ Milwaukee computers, such as home computers, is also subject to termination. Certain licensed software, such as remote-access programs, may be copied to home computers with proper approval of designated IT personnel. Upon termination, personnel must remove any such programs from his or her computer and destroy any backup copies.

No personal software will be installed on any Employ Milwaukee computer. Any deviation from this policy must have written approval from designated IT personnel. Should you consider it necessary or believe it to be desirable for Employ Milwaukee to acquire a particular software package, you must receive approval from designated IT personnel. In addition, designated IT personnel must be consulted during the selection process to evaluate technical considerations. Any Employ Milwaukee purchased software is to be purchased through designated IT personnel for inventory control and installation. Only software that has been through this selection process will be installed on Employ Milwaukee computers.

Workstation Security

Use of Employ Milwaukee's workstations (including, but not limited to, personal computers, laptops, "smartphones", etc.) is restricted to authorized personnel. Personnel in possession of such devices owned by Employ Milwaukee, or in possession of devices containing Employ Milwaukee's information, must take precaution to protect and control these devices from unauthorized physical access, loss, or theft. Personnel must not leave these devices unattended in unprotected public areas or during transit.

Facility Access Controls

Physical access to information systems and the facilities in which they are housed must be restricted to properly authorized individuals.

Such restrictions must:

- safeguard information system facilities and the equipment therein from unauthorized physical access, tampering, and theft,
- control and validate access based on role or function,
- support restoration of lost data under the contingency plans,

Repairs and modifications to the facilities physical security components should be documented.

Security Management System

Information security is to be managed through a process designed to prevent, detect, contain, and correct violations of the information security policies.

IV. PROCEDURES

Lost Device Procedures

In the event a device is lost or stolen, the workforce member assigned that device must immediately report the incident at the time of discovery to designated IT personnel.

Workforce members must not discuss the incident with other personnel, clients, donors, law enforcement, or anyone else until they have received explicit instructions to do so from designated IT personnel or from the CEO.

The security management process must include:

- analysis of risks posed to information systems,
- treatment of identified risks,
- sanctions for violations of information security policies, and
- proactive review of information system activity

RECISSIONS: N/A
BOARD APPROVAL DATE: 8/26/21