WELDO
Rebuilding Lives

Access Control Policy

1 Purpose

This policy is to ensure that the WELDO has implemented the controls needed to limit access to computing resources to only those people who are authorized to use the resources.

2 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at WELDO. This policy applies to all computing equipment that is owned or leased by WELDO.

3 Policy

3.1 Data owners or their designated representatives shall ensure appropriate procedures are documented, disseminated, and implemented to ensure compliance with this policy.

3.2 All individuals must have authorization from the Data owners or their designation representatives prior to being granted or modifying access to IT resources that store, process or transmit confidential or protected data.

3.3 Access rights shall be granted based on business requirements.

- Access rights shall be properly authorized and documented by Data owners Access rights shall also be documented by WELDO.
- WELDO shall implement a process for disabling employee user-accounts when the account holder has left WELDO employment or moved to a different site, or when a user's access requirements to the data change (e.g., job assignment change).
- Access rights to confidential or protected data shall not exceed the minimum necessary for a user's assigned duties.
- Departmental procedures shall be developed and implemented for authorizing user Access to IT resources that store, process or transmit confidential or protected data.

3.4 All users shall be assigned unique user identifier(s) (or login name(s)) for the purposes of authenticating to IT resources.

- Users shall not share assigned unique system identifiers (or login names) with any other person.
- Anonymous access, including the use of guest and public accounts, to any IT resource that store, process or transmit confidential or protected data is prohibited.

- Unique user identifiers (or login names) shall be used with a password for authentication to an IT resource that stores, processes or transmits confidential or protected data.
- Passwords shall not be shared with any other person.

3.5 System and application password configurations shall meet the minimum requirements according to section 4 mentioned below.

3.6 User's access to IT resources shall be terminated when access is no longer necessary or when determined by management (including when the relationship between the user and WELDO is terminated).

- The HR Department is responsible for making appropriate and timely requests to the IT Department for user's account deactivation.
- A formal termination process shall be used and shall include documentation and verification.

3.7 Data owners, administrators and senior managers shall participate in user access right reviews at regular intervals using a formal process.

4 Passwords

The best security against a password incident is to follow a sound password construction strategy. WELDO strongly suggests users adhere to the following guidelines on password construction.

4.1 Passwords should: be at least 8 characters, be a mix of letters, numbers and special characters (punctuation marks and symbols), be a mix of upper and lower case characters, not utilize words that can be found in a dictionary, not be an obvious keyboard sequence (i.e., qwerty), Not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

4.2 Passwords should be considered confidential data and treated with the same discretion as any of the company's proprietary information. The following guidelines apply to the confidentiality of passwords.

- Users should not: disclose their passwords to anyone, share their passwords with others (co-workers, supervisors, family), write down their passwords or leave them unsecured, check the "save password" box when authenticating to applications, use the same password for different systems and/or accounts, send passwords via email, re-use passwords in order to maintain good security passwords should be periodically changed. This limits the damage a hacker can do as well as help frustrate brute force attempts.

- At a minimum, users must change passwords every 90 days.
- On termination of user employment all access to the company’s systems and external systems will be revoked.

5 Enforcement

Violations of this policy will result in appropriate disciplinary measures in accordance with WELDO regulations.

Any individual who suspects a violation of this policy may report it to the Data Protection Officer through email to dpo@weldo.org.